Logicube Talon® User's Manual

Logicube, Inc.
Chatsworth, CA 91311
818 700 8488

P/N MAN-TALON
Version: 1.8
Date: 10/07/10

Limitation of Liability and Warranty Information

Logicube Disclaimer

LOGICUBE IS NOT LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO PROPERTY DAMAGE, LOSS OF TIME OR DATA FROM USE OF A LOGICUBE PRODUCT, OR ANY OTHER DAMAGES RESULTING FROM PRODUCT MALFUNCTION OR FAILURE OF (INCLUDING WITHOUT LIMITATION, THOSE RESULTING FROM: (1) RELIANCE ON THE MATERIALS PRESENTED, (2) COSTS OF REPLACEMENT GOODS, (3) LOSS OF USE, DATA OR PROFITS, (4) DELAYS OR BUSINESS INTERRUPTIONS, (5) AND ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE (OR FROM DELAYS IN SERVICING OR INABILITY TO RENDER SERVICE ON ANY) LOGICUBE PRODUCT.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ALL PRODUCTS. HOWEVER, THE CUSTOMER IS RESPONSIBLE TO VERIFY THAT THE OUTPUT OF LOGICUBE PRODUCT MEETS THE CUSTOMER'S QUALITY REQUIREMENT. THE CUSTOMER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCT AND/OR SOFTWARE, OR HARDWARE PROBLEMS, CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY CUSTOMER, EITHER UNDER WARRANTY OR ON A TIME AND MATERIALS BASIS.

Warranty

LOGICUBE PROVIDES A BASIC ONE-YEAR PARTS AND LABOR WARRANTY FOR ALL OF ITS PRODUCTS (EXCLUDING CABLES, ADAPTERS AND OTHER "CONSUMABLE" ITEMS). A TWO-YEAR EXTENDED WARRANTY IS ALSO AVAILABLE FOR AN ADDED COST. TELEPHONE AND EMAIL SUPPORT IS AVAILABLE FOR THE LIFE OF THE PRODUCT AS DEFINED BY LOGICUBE.

RoHS Certificate of Compliance

LOGICUBE PRODUCTS COMPLY WITH THE EUROPEAN UNION RESTRICTION OF THE USE OF CERTAIN HAZARDOUS SUBSTANCES IN ELECTRONIC EQUIPMENT, ROHS DIRECTIVE (2002/95/EC).

THE ROHS DIRECTIVE PROHIBITS THE SALE OF CERTAIN ELECTRONIC EQUIPMENT CONTAINING SOME HAZARDOUS SUBSTANCES SUCH AS MERCURY, LEAD, CADMIUM, HEXAVALENT CHROMIUM AND CERTAIN FLAME-RETARDANTS IN THE EUROPEAN UNION. THIS DIRECTIVE APPLIES TO ELECTRONIC PRODUCTS PLACED ON THE EU MARKET AFTER JULY 1, 2006.

Logicube Declaration of Conformity

CE

LOGICUBE DECLARES THAT THIS PRODUCT MEETS ALL APPROPRIATE EUROPEAN UNION (EU) HEALTH, SAFETY, AND ENVIRONMENTAL REQUIREMENTS, WHICH ENSURE CONSUMER AND WORKPLACE SAFETY. IT IS IN COMPLIENCE WITH ALL REQUIREMENTS AND PROVISIONS OF DIRECTIVE 89/336/EEC, AND ALL OTHER RELEVANT DIRECTIVES.

PLEASE CONTACT LOGICUBE, INC. FOR A COPY OF THIS DECLARATION.

Table of Contents

1. Introduction to the Forensic Talon®

Introduction

Thank you for purchasing the Logicube Forensic Talon® Kit. With proper use, this kit will provide you with accurate HDD capturing for years to come.

The Logicube Forensic Talon® is a drive-to-drive duplication device. Typically, a suspect hard drive and a destination drive will be connected to the unit. Within minutes of starting the process, the contents of the suspect drive are accurately copied over to the destination drive for further examination. Handling of the suspect drive is held to a minimum with zero alteration of its contents.

Designed with the Forensics investigator in mind, the system ensures that proper evidence capture procedures are maintained, speeding up the process significantly with little room for error.

The Forensic Talon® is a successor to our highly acclaimed MD5™. It represents the 5th generation in Computer Forensic-related tools from Logicube.

Features

- Capturing Speeds nearing 4GB/min – Achieved through the use of synchronized UDMA-5 engines.
- Ability to compute SHA-256 or MD5 Hash in real time (at full Capturing speed).
- Keyword search capabilities – Search for hundreds of words concurrently on a hard drive. Either during the capture process, or on a single drive. Specify: upper-case, case-insensitive, Unicode, start of sector, regular expression.
- DD image capture mode – Capture a suspect's hard drive to multiple DD image files. User specified file size of: 650MB, 2GB, and 4GB, for later archiving on to CD-R's, Jaz drives, and DVD-R's respectively.
- Removable Compact Flash slot (64MB CF card included) – Stores keyword lists, software updates, reports etc.
- Fully integrated QWERTY keypad – For easy entry of file names, user password, keywords, etc.

Using this guide

This user guide is made up of 12 sections:

- Introduction
- Getting Started (Fast Start)
- Cloning Modes and Settings
- Other Modes
- Using the Clone Card Pro™
- Using the USB Write PROtect™ Adapter
- Using the RAID I/O Adapter™
- Using the GPStamp™
- Keyword Searching
- Compact Flash (CF) Drive
- Software Loading Instructions
- Reference/FAQ's

Please read Modules 1. Introduction, and Module 2. Getting Started before attempting a drive capture. It is recommended that you practice with a scratch drive to fully appreciate the procedures.

System description – Forensic Talon Kit

The Forensic Talon® Kit is packed in a rugged, watertight carrying case. Inside, you will find the following components:

- The Logicube Forensic Talon® with power adapter.
- A 64MB Compact Flash Card that includes:
  - A backup copy of the current Forensic Talon® software.
  - A text file that contains sample Keyword Lists.
- Sets of standard length (5" and 9") drive power cables (used to connect the suspect and destination drives to the unit).
- HDD (Hard Disk Drive) data cables to connect suspect drive to Forensic Talon®; two lengths.
- Two Serial ATA cables, one short and one long, for attaching Serial ATA drives to your Logicube Talon®.
- An extra long (18") drive data cable to reach a suspect drive still mounted in a PC chassis.
- One 2.5" drive adapter to allow the connection of laptop drives.
- One Logicube CloneCard Pro™– A PCMCIA adapter with a floppy disk containing a client application. This is used for capturing data from notebook PCs.
- A "Mini-B" USB cable that allows the unit to be connected to the USB port of a PC.
- A Brother MW-120™ portable thermal printer, which also comes with an AC power supply, parallel cable, internal battery, carrying case and documentation.
- 100 sheets of thermal printer paper.

  NOTE: Please contact Logicube if extra paper is needed.
- A flashlight and screwdriver.
- A CD-ROM that includes:
  - A utility program to load the Forensic Talon® with new software.
  - A backup copy of the current Forensic Talon® software.
  - Extra copies of all files found on the Compact Flash Card.

- Another CD-ROM that includes:
  - Write PROtect™ Cloning software to capture suspect drives through the USB port.
- A hard plastic carrying case.

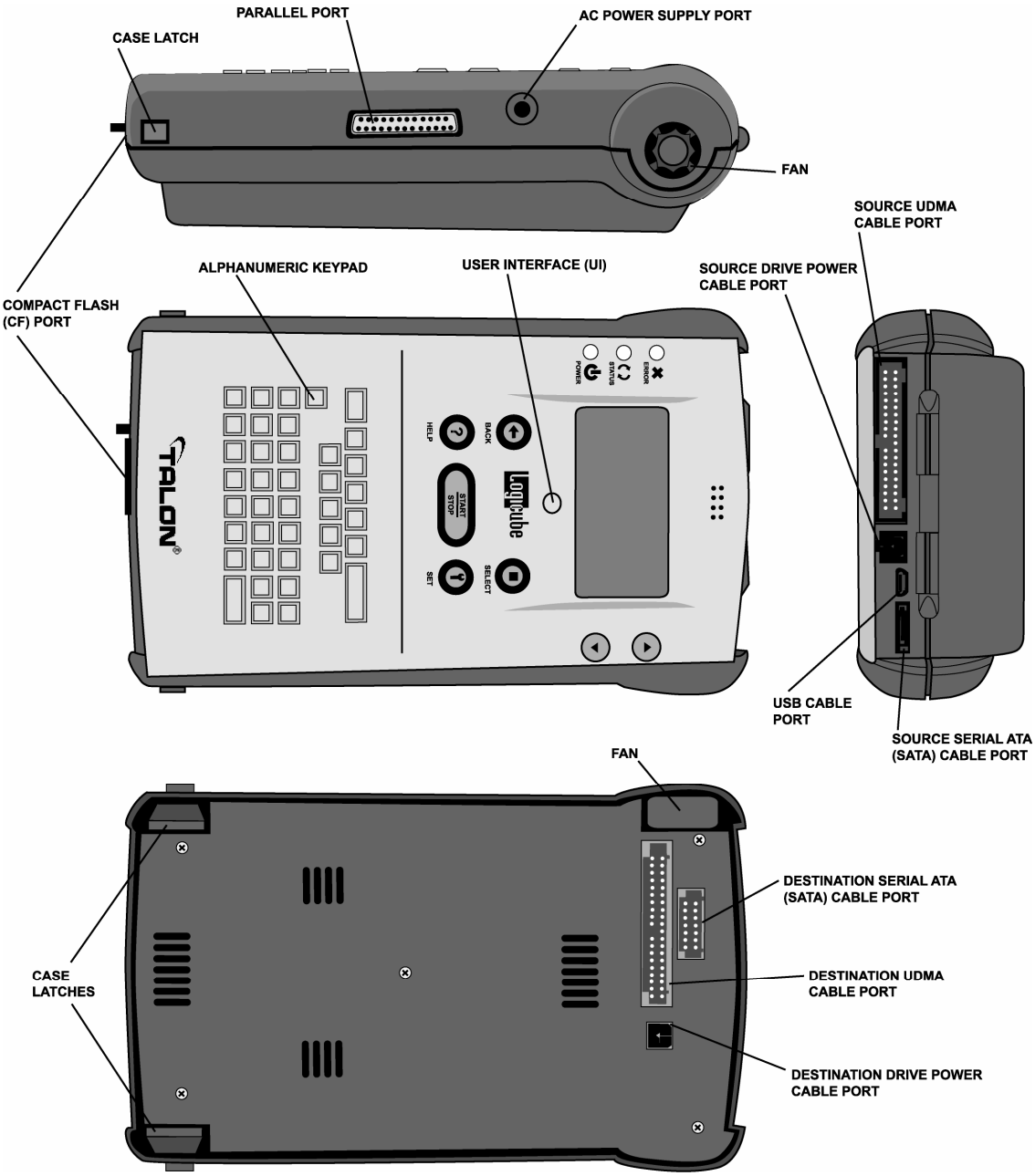
  NOTE: It is recommended that you always use the carrying case to store and carry the unit.
- This manual.

System description – Forensic Talon Standalone

The Forensic Talon® Standalone unit comes in a rugged, canvas carrying bag. Inside, you will find the following components:

- The Logicube Forensic Talon® with power adapter.
- A 64MB Compact Flash Card that includes:
  - A backup copy of the current Forensic Talon® software.
  - A text file that contains sample Keyword Lists.
- Sets of standard length (5” and 9”) drive power cables (used to connect the suspect and destination drives to the unit).
- HDD (Hard Disk Drive) data cables to connect suspect drive to Forensic Talon® two lengths.
- Two Serial ATA cables, one short and one long, for attaching Serial ATA drives to your Logicube Talon®.
- A “Mini-B” USB cable that allows the unit to be connected to the USB port of a PC.
- A flashlight and screwdriver.
- A CD-ROM that includes:
  - A utility program to load the Forensic Talon® with new software.
  - A backup copy of the current Forensic Talon® software.
  - Extra copies of all files found on the Compact Flash Card.
- Another CD-ROM that includes:
  - Write PROtect™ Cloning software to capture suspect drives through the USB port.

Figure 1. Forensic Talon®



Caution: Incorrectly connecting the suspect drive to the system can result in data on the suspect drive to be lost forever.

Caution: Never place a suspect drive INSIDE the Logicube Talon®Forensic Talon®Forensic Talon® as data erasure can result.

Caution: Never place a suspect drive into any other Logicube products (e.g. Sonix™) that are used for Operating System cloning).

2. Getting Started (Fast Start)

Applying power to the Logicube Talon™

The Logicube Talon® is able to detect whether an IDE (parallel) or Serial ATA (SATA) drive is attached to the Source or Destination position. The unit is capable of cloning to/from a SATA drive to an IDE drive and vice versa (as well as IDE to IDE and SATA to SATA).

NOTE: Never attach both an IDE and SATA drive to the Source or Destination position. The unit can only handle one drive on each position.

Before applying power perform the steps listed below.

Connecting a Parallel (IDE) Drive

1. Open the Logicube Talon® by pressing on the two latches at the base of the unit and lifting the top. You will notice three connections: One for a flat cable (the drive data cable) and another for a small drive power cable. Underneath is the third connector for the Serial ATA cable.

   Note: See Figure 2, Connecting a Destination drive to the Logicube Talon® through 5" Data/Power cables.

2. Connect a Destination hard drive and close the Logicube Talon®.

3. Plug in the set of 9" cables, to the connections found on the back of the Logicube Talon®.

   Note: See Figure 3, Connecting a Source drive to the Logicube Talon® through 9" data/power cables.

4. Connect the Source drive to these cables.

   Note: The internal drive is always referred to as the **Destination** (or **Evidence**) drive and the outside drive is always referred to as the **Source** (or **Suspect**) drive.

5. Connect the external power supply to the Logicube Talon® and power-up the unit. In 2 – 3 seconds, the main "Splash" screen appears.

Figure 2. Connecting an IDE (parallel) Destination Drive

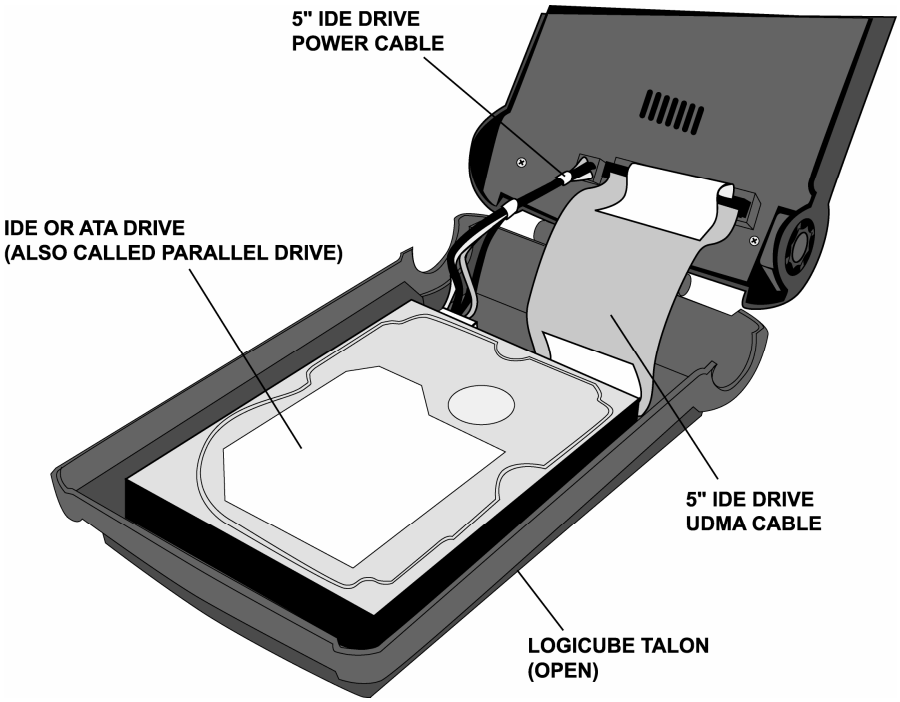
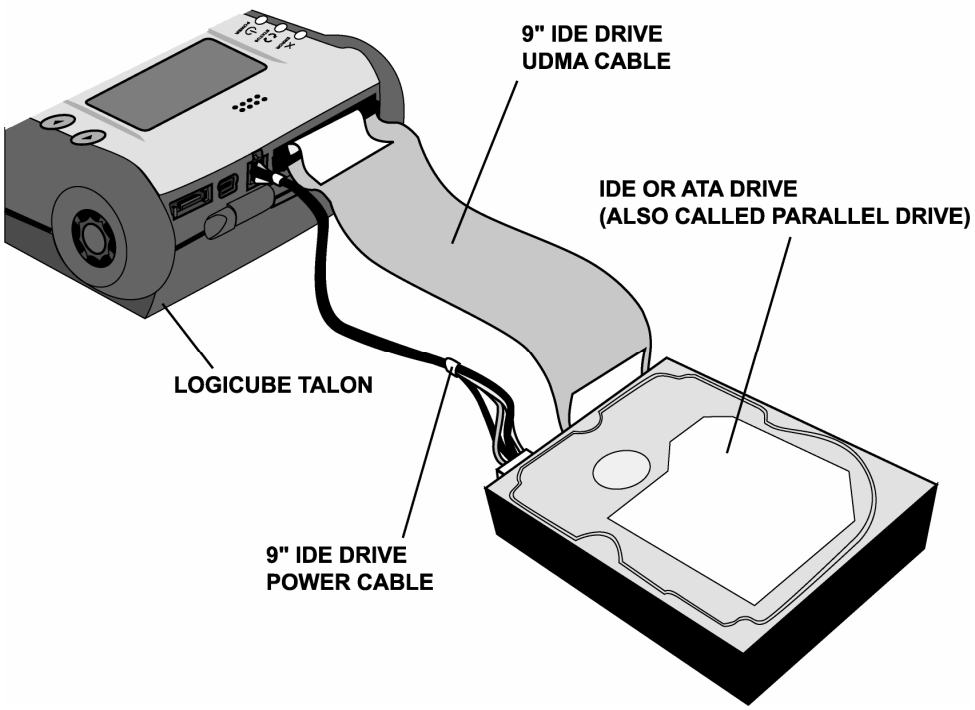


Figure 3. Connecting an IDE (parallel) Source Drive



Parallel Port

The parallel port on the side of the Talon® serves two main purposes. It downloads software updates via DOS and it also allows connectivity of the Talon® to peripheral devices like the Portable Forensic Lab™ (PFL) or GPStamp™.

Connecting a Serial ATA (SATA) Drive

1. Open the Logicube Talon® by pressing on the two latches at the base of the unit and lifting the top. You will notice three connections: One for a flat cable (the drive data cable) and another for a small drive power cable. Underneath is the third connector for the Serial ATA cable.

   Note: The UDMA drive data and power cables should be removed from the Talon when a SATA drive is connected. This will ensure optimal cloning speeds.

   Note: See Figure 4, Connecting a Destination drive to the Logicube Talon® through a 5" SATA cable.

2. Connect a Destination hard drive and close the Logicube Talon®. Make sure that Pin 1 is properly aligned.
3. Plug in the long SATA cable to the connections found on the back of the Logicube Talon®.

Note: See Figure 5, Connecting a Source drive to the Logicube Talon® through a 9" SATA cable.

4. Connect the Source drive to this cable.

   Note: The internal drive is always referred to as the **Destination** (or **Evidence**) drive and the outside drive is always referred to as the **Source** (or **Suspect**) drive.

5. Connect the power supply to the Logicube Talon® and power-up the unit. In 2-3 seconds, the main display appears.

Connecting other types of drives

Logicube sells specialized adapters that allow other types of drives to be connected to the Logicube Talon®. Such drives include 2.5" laptop drives, 1.8" laptop drives (e.g. Toshiba "iPod™" drives, compact Flash (CF) drives and USB drives.

Other specialized adapters are also available. If you are unsure about the type of drive that you have, please contact Logicube Technical Support for assistance.

Note: SCSI drives cannot be connected directly to the Logicube Talon®. Please refer to **Chapter 6, Using the USB Port**, for cloning SCSI drives.

Figure 4. Connecting a Serial ATA (SATA) Destination Drive.

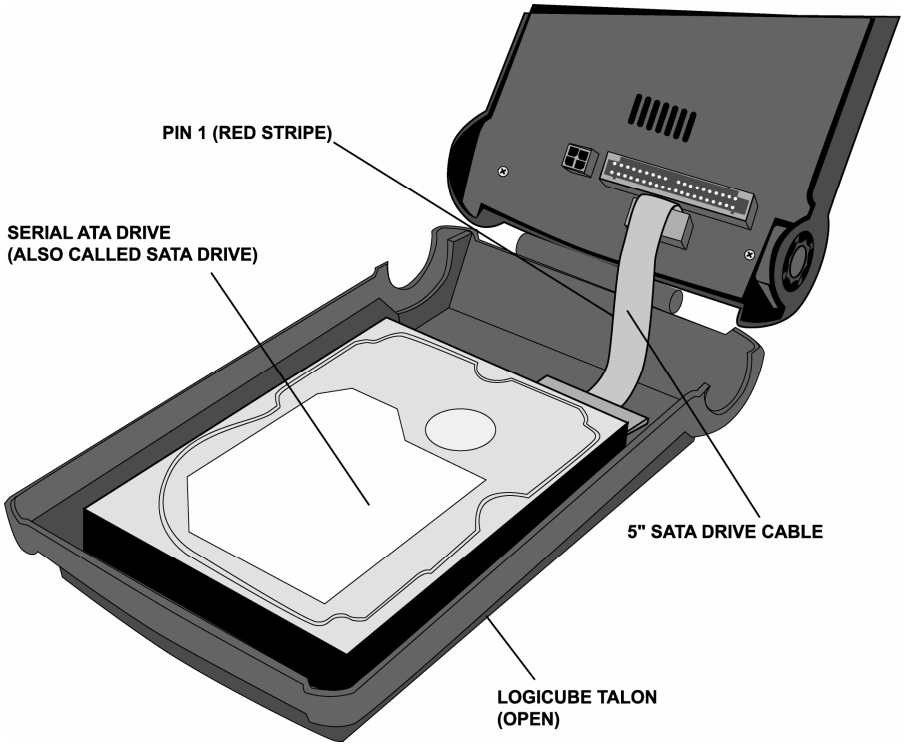
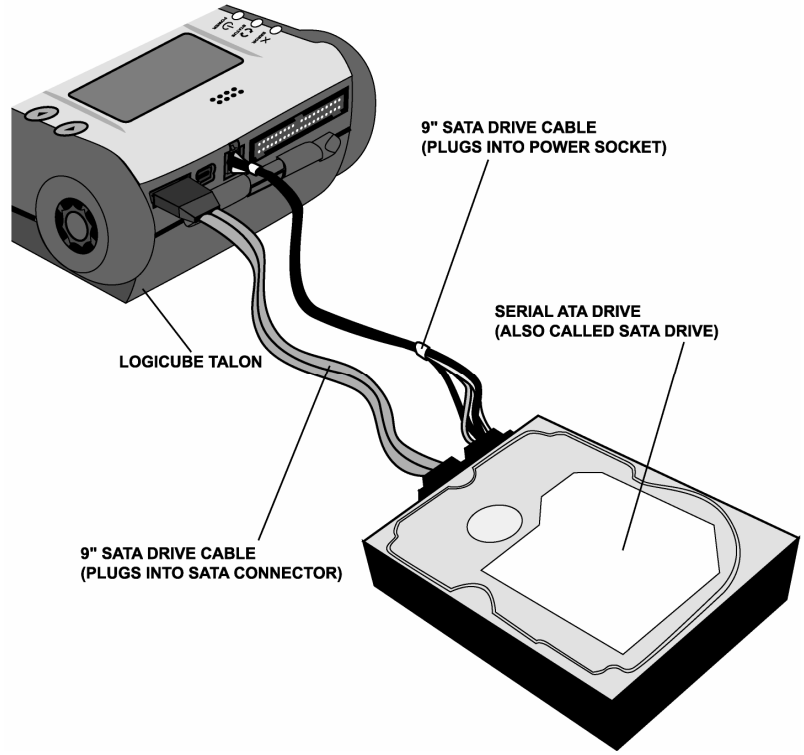


Figure 5. Connecting a Serial ATA (SATA) Source Drive.



The user interface

The user interface (UI) has been designed with the professional in mind. It is fast, responsive, and to the point; which means it requires very few key strokes to achieve a desired action.

"Shortcut" buttons (available at all times)

NOTE: Refer to Figure 3 as you read the information below.

- **START/STOP** Button – Press it twice to begin a cloning operation using the current settings; press the START/STOP button in mid process to abort it. A single key stroke presents a preview screen where you can see the current setting, and decide whether to press it again to begin the capture, or back out to reconfigure.
- The "**Help**" **("?")** button provides context sensitive help and is active at all times. Press it to get specific help on the current screen. If the selection cursor is on the screen, pressing the Help button will retrieve specific help for that item pointed to. Press the help button again to return to the current screen.
- The "**Set**" button is the third "shortcut" button. It brings you to the settings screen where you can change capture modes and other settings of the unit.

"Soft" Buttons

The two "Soft" buttons are directly under the LCD display. The button functions change depending on the labels displayed above them.

> **Note:** Labels are always enclosed by angular brackets (<>). When no labels are displayed, they function as navigational buttons.

The right button functions as "**Select**" or "toggle" and is used to select an option, to move through multiple available options, or to select a sub-menu.

The left button is the "**Back**" button. This button is used to go "up" in the menu system or to cancel out of a given operation.

Scroll buttons

The two scroll buttons are active when the right side of the screen displays the scroll arrows. This occurs when the amount of information to display exceeds the screen size. Menus are also scrollable

Alphanumeric Keypad

The alphanumeric keypad is laid out like the keypad on your PC or typewriter. It is used for labeling capture sessions, entering passwords and other functions.

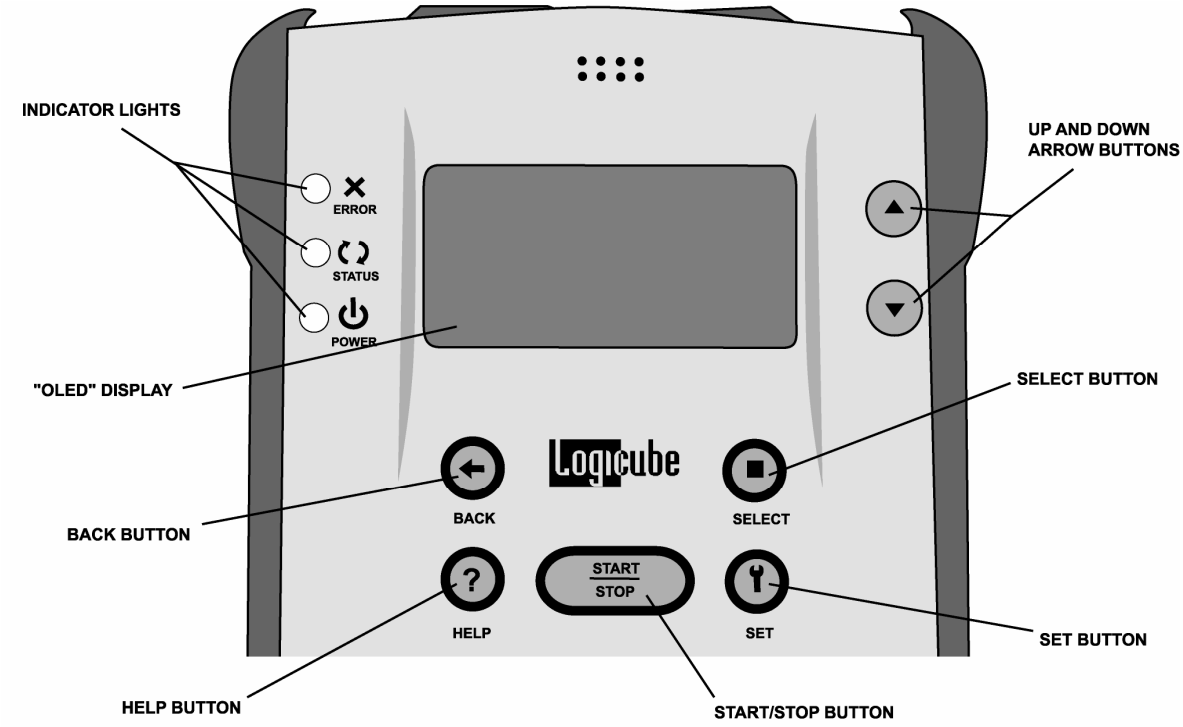
Indicator Lights

The **POWER** indicator light remains on while the Logicube Talon® is receiving power.

The **STATUS** indicator is lit during cloning operations and any operation that accesses the Source or Destination drive. It will flash as data is transferred from one drive to the other.

The **ERROR** light will come on if a problem is encountered during cloning or any other operation. If this occurs, check the screen for an error message and instructions on what to do next.

Figure 6. Buttons and Interface



3. Drive Capture Modes and Settings

Main Screen

The main menu screen appears when the Logicube® is first powered up. It displays the Title Screen and two menu options: **About** and **Drives**.

About Screen

Select the About Screen by pressing the Back button. It will display the serial number of your unit along with the software and firmware versions that are loaded. In addition, the About screen provides contact information for Logicube Technical Support.

To return to the main menu, simply press the Back button at any time.

Drive Info

Select the Drive Info screen by pressing the Select button. Another screen will come up asking you to select either the **<Source>** or **<Dest.>** drive (use the "soft" buttons to make your choice). The unit will then access the drive selected and report back the drive's model number, capacity, geometry and other information.

To return to the main menu, you may select **<Done>** by pressing the back button at any time.

Screen Saver

After 25 seconds of inactivity, the Logicube Talon® display will switch to a screen saver. This is designed to extend the life of the OLED display used by the unit.

Pressing any one of the UI buttons will switch the display back to normal.

Modes of Operation

The Logicube Talon® supports two different operations to clone data from a suspect drive. They are **Native Capture** and **DD Image Capture**. These modes are found in the Mode Setting Menu along with several other operations. The different modes of operation are briefly described below.

NOTE: Each time the Logicube Talon® is powered off the cloning mode and preference settings are returned to their factory defaults.

The following Modes of Operation are found in the Mode Setting Menu:

- **Capture (Native)** – This process captures all data from the source drive to the destination drive. This mode is called a "Native Capture" since data is captured at the sector level to another dedicated destination drive.
- **Drive Defect Scan** – This operation performs a surface scan of the drive media using the drive controller to verify the media, and detect bad or "weak" sectors. This mode is described in **Chapter 4. Other Modes**.
- **WipeClean™ Dest.** – This is used to erase all data on the destination drives prior to a Native Capture. This mode is described in **Chapter 4. Other Modes**.
- **Calculate HASH** – This is used to compute SHA-256 or MD5 values of the source or destination drive at extreme speeds, and is useful for an "after the fact" verification of a drive. This mode is described in **Chapter 4. Other Modes**.
- **USB Drive Mode –** This mode needs to be engaged when attempting a USB capture through the integral USB port. This mode is described in **Chapter 6. Using the USB Write PROtect™ Adapter**.
- **Keyword Search –** Used to perform a binary keyword search on a given drive. This mode is described in **Chapter 5. Keyword Search**.
- **DD capture (650 MB)** – This mode of Capturing creates a sub-directory per drive captured, with DD style files of size 650 MB each. These files are directly accessible by popular Forensic analysis software tools, such as, Encase, FTK, and ILook. The 650MB size is designed to allow archiving onto CD-R's.

- **DD capture (2 GB)** – Same as above, except each file is 2GB large. This size is compatible with archiving onto Jaz drives.
- **DD capture (4 GB)** – Same as above, except each file is 4GB in size. This size is compatible with archiving onto DVD-R's.
- **Audit Trail** – This mode is used to verify the authenticity of a report that is stored on the Compact Flash drive.

Capturing a Drive

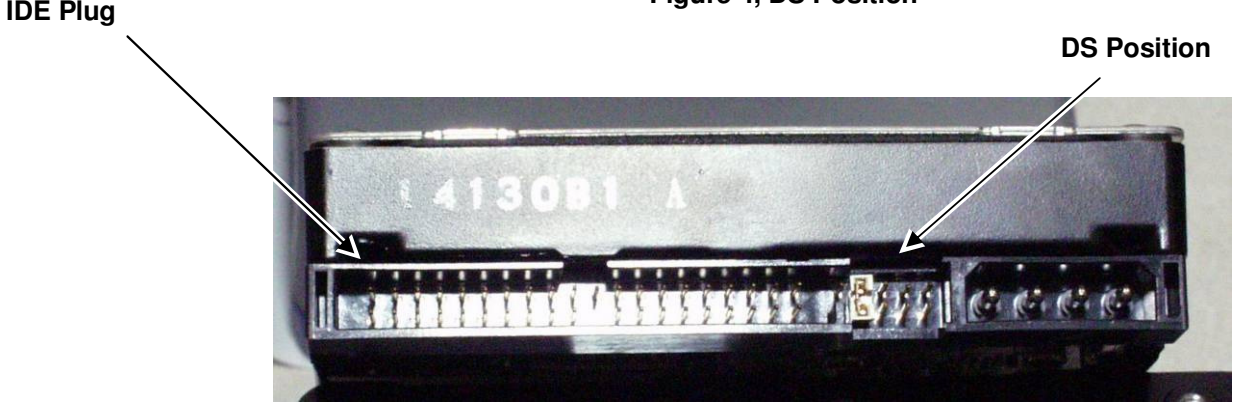
Connect the drives as previously described. Make sure the target drive is equal to or larger in capacity to the suspect drive (source drive).

Note: In order for a capture to work, most drives must be configured as a master drive. If you are going to capture a drive that is used as a slave, move the jumper to the master position. Before moving a jumper note its position so you can return the suspect drive to its original state when the capture operation has been completed.

Note: There are several drives that do not follow the requirement stated above. Those drives are:

- **Western Digital** – Most Western Digital drives require that the jumpers be removed for a capture to work. The exception to this requirement is for the Western Digital "Xpert" series hard drives (an older manufactured version) where the jumper is set to the master position.
- **Quantum** - The jumper must be placed in the "DS" position. The "DS" position is adjacent to the IDE plug, see figure 4.

Figure 4, DS Position



To perform a (Native) Capture

1. Make sure that the Source and Destination drives are attached to the unit and power is applied.
2. From anywhere in the menu system press the <Set> button to enter the Settings menu.
3. Scroll to the top item called “Mode” and press the <Select> button. The Mode screen appears.
4. Scroll to Capture and press <Select> again.
5. Scroll through the optional preferences – Verify, On Error, and Speed - and modify them as needed using the Select button to toggle between the different settings for each.

   NOTE: See the Optional Preference Settings section of this chapter for more information on these preference settings.
6. Press the <**START**/**STOP**> button twice.
7. The Talon® will access the CF Drive, then the following message will appear: “KEYPAD ENTRY: Enter Log file name. Press Select when done”.
8. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Select button when finished.
9. If the Destination drive has not been erased with the Wipeclean™ Dest. Mode, the unit will ask if you wish to erase the Destination drive. Press the Select button for <Yes> or the Back button for <No>. If <Yes> is chosen, the unit will completely wipe the destination drive before it begins to capture data.

   NOTE: The final capture report will state whether or not the Destination drive has been properly erased.
10. The unit will “Mirror” Clone all of the data from the Suspect drive to the Destination drive.
11. After the data has been captured, if the destination drive was not erased, the unit will ask if you wish to erase the remainder of the Destination drive. Press the Select button for <Yes> or the Back button for <No>. If <Yes> is chosen, the unit will completely wipe the rest of the destination drive.

    NOTE: The final capture report will state whether or not the Destination drive has been properly erased.

12. If the Printer was set to “Yes”, the user will be prompted to connect the printer and make sure that it is powered up and online. Press SELECT to print or BACK to skip printing.

    NOTE: Please refer to “*Printing a Report*” on page 20 for more printing options.

13. A copy of the Final Capture Report is written to the CF Drive. It is titled <Log file name>.LOG. The report can be accessed and printed from Windows, if the Talon® unit is connected to a PC via USB.

    NOTE: Please refer to *“Connecting the CF Drive to Windows via USB”* on page 36.

14. The capture ends with a “Capture Successful” message. It also displays the SHA-256 or MD5 Hash value for the Source and Destination drives together.

To Perform a DD image Capture

1. From anywhere in the menu system press the <Set> button to enter the Settings menu.
2. Scroll to the top item called “Mode” and press the <Select> button. The Mode screen appears.
3. Scroll to one of the DD imaging options and press <Select> again. One of three file sizes can be selected: 650MB, 2GB or 4GB.
4. Scroll through the optional preferences – Verify, On Error, and Speed - and modify them as needed using the Select button to toggle between the different settings for each.

   NOTE: See the **Optional Preference Settings** section of this chapter for more information on these preference settings. Also, see the **Special Settings** section below.

5. Press the <START/STOP> button twice. The Talon® will briefly access the CF Drive.
6. The following message will appear: “Continuing will overwrite a portion of your Destination drive. Are you sure?” Press the Select button for <Yes>.
7. The Destination Drive needs to be formatted before data capture is possible. If it hasn’t been formatted yet, a prompt will come up. Choose <Yes> to format the drive.

NOTE: See the Special Settings section below for more information on managing the Destination drive.

8. You will then be prompted to enter a Case file name using the keypad. Up to 8 characters are allowed following traditional DOS naming conventions.

   NOTE: If a Case file already exists on the destination drive (i.e. from a previous DD Image capture) the unit will not allow you to enter the same file name again.

9. A sub-directory (by the same name) will be created under the root directory on the destination drive.

10. The capturing process will create as many files as necessary within this sub-directory, with increasing extension numbers (e.g. my_disk.001, my_disk.002, etc.)

11. At the end of the process, a file with the **.log** extension is created and placed in the same sub-directory. The file is also written to the CF Drive. It includes (among other things), the SHA-256/MD5 Hash values of all captured DD files or the entire Source Drive. Refer to the **Special Settings** section below.

12. If the Printer was set to "Yes", the user will be prompted to connect the printer and make sure that it is powered up and online. Press SELECT to print or BACK to skip printing.

    NOTE: Please refer to "*Printing a Report*" on page 20 for more printing options.

13. The capture ends with a "Capture Successful" message.

Special Settings for DD Image Capture Mode

Verify Disk or File

For DD Image Capture Mode, the Verify Setting has some optional settings that are not available in any other mode. The settings available are:

256 + File - This is the default setting for verification and uses special hardware to compute SHA-256 values for each individual DD Image file.

256 + File + V - This setting behaves like 256 + File, except that it also reads back captured data and compares it to the Source drive.

256 + Disk - This setting uses special hardware to compute the SHA-256 value for the entire Source drive.

256 + Disk + V- This setting behaves like 256 + Disk, except that it also reads back captured data and compares it to the Source drive.

MD5 + File - This setting uses special hardware to compute MD5 values for each individual DD Image file.

MD5 + File + V - This setting behaves like MD5 + File, except that it also reads back captured data and compares it to the Source drive.

MD5 + Disk - This setting uses special hardware to compute the MD5 value for the entire Source drive.

MD5 + Disk + V- This setting behaves like MD5 + Disk, except that it also reads back captured data and compares it to the Source drive.

None- No verification. This setting is only recommended for non-Forensic cloning operations.

Manage Destination

DD Image Capture mode also uses a special menu called “Manage Dest.”. This menu allows the Destination drive to be prepped before running a DD Image capture. The settings available are:

Format Dest. – This function formats the destination drive with a single FAT32 partition. This is necessary before DD Image files can be copied to the drive. When Format Dest. Is activated, the following prompt appears:

“Reformatting the Drive! All data on your Internal Drive will be lost! Continue?

Press the Select button for <Yes>, the display will say “Zeroing first FAT” and “Zeroing second FAT” as it formats the drive. After 30 – 60 seconds the drive will be formatted, (the time varies by drive size).

Press the Back button for <No>, the display will then go back to the Manage Dest. Menu.

Scandisk – This function checks the Destination Drive for proper formatting. It also

makes sure that the FAT32 partition is not corrupt. It functions much like Microsoft Windows Scandisk or Chkdsk.

Press the Select button to run Scandisk. After 30 seconds, it will display a list of errors, if any.

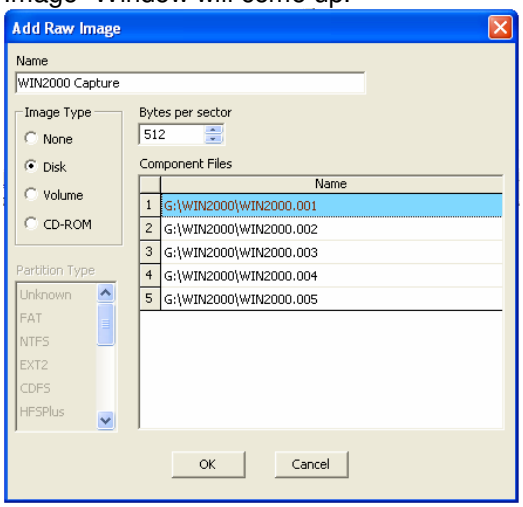
Browse Dest. – If the Destination Drive is formatted with a FAT32 partition, Browse Dest. Will allow the user to navigate directories on the drive. It will also show the size of files on the drive. Use the Arrow keys and Select button to navigate the directories.

Loading DD Image files into Encase™

Once the DD Image files are captured to a Destination drive, they can be easily loaded into a Forensic Investigative tool like Encase™.

NOTE: These instructions are for Encase™, by Guidance Software. Other Investigative software products may follow a similar procedure. Consult your software's manual for more information.

1. Attach the Talon® to the PC via the USB Port, (please refer to the procedure for "Destination Drive Analysis" on page 27).
2. Open Encase™ and start a new case.
3. Go to **File** – **Add Raw Image**. The "Add Raw Image" Window will come up.



4. Set **Image Type** to **Disk** and leave **Bytes per Sector** at **512**.
5. Right-click in the **Component Files** box. Choose "**New - Insert**".
6. Browse to the location of your DD Image files, they should be in the drive labeled

"Logicube_dd" and located in a folder with the case name that you entered during the Talon® capture process.

7. Select all DD Image files this way: Select the last file, then hold down the SHIFT key while clicking the fist file.

8. Click "OK" to add the files to the "Add Raw Image" box.

9. You may need to click and drag the files up and down in order to put them in descending order (i.e. *.001, *.002, *.003, etc.).

10. Click **OK**. Encase will then put the files back together into a complete image of the disk.

Printing a report

At completion of a capture, you might want to print a report. You must keep the Forensic Talon® powered on in order for it to retain the report information from the last session.

NOTE: Logicube Talon® Forensic Kits include a Brother MW-120 portable thermal printer.

Printing with the included Brother (thermal) Printer

1. Connect the Brother printer to the Forensic Talon® using the special serial cable included with the kit.

2. Power the printer using the printer power adapter.

   CAUTION: Don't confuse this power adapter with the Forensic Talon® power adapter. Press the power button on the printer until it lights up

3. Make sure that the printer is loaded with A7 size thermal paper. See the Brother User Manual for paper loading instructions.

   NOTE: The Brother printer cannot use plain paper. It uses thermal paper only.

4. On the Forensic Talon®, press the <**Set**> button to go to the Settings menu. Scroll down to the Printer option and press the <**Select**> button
5. Scroll to the "Select reports…" item and press the <**Select**> button.
6. Scroll to the "Print Last Session" item and press the <**Select**> button.
7. A prompt will come up asking the user which printer is connected to the unit. Choose "**BROTHER MW-120**".

   NOTE: Once a printer is chosen, the user will not be prompted again until the unit is rebooted.

8. Follow the instructions on the screen. A report should now print.

Every operation performed with the Talon® also writes a copy of the report to the CF Drive. This report can be easily accessed in Windows and printed from a text editor like Notepad.

Printing with the Pentax (thermal) Printer

Forensic Talon® kits sold prior to January 2007 included a Pentax Pocketjet 200 portable thermal printer. To use this printer:

1. Connect the Pentax printer to the Forensic Talon® using the special cable included with the kit.
2. Power the printer using the printer power adapter.

CAUTION: Don't confuse this power adapter with the Forensic Talon® power adapter. Press the power button on the printer until it lights up

3. Load a sheet of the special thermal paper into the printer. Make sure that the "shiny" side of the paper faces down. The printer will engage and advance the paper slightly.

   NOTE: The Pentax printer cannot use plain paper. It uses thermal paper only.

4. On the Forensic Talon®, press the <**Set**> button to go to the Settings menu. Scroll down to the Printer option and press the <**Select**> button
5. Scroll to the "Select reports…" item and press the <**Select**> button.
6. Scroll to the "Print Last Session" item and press the <**Select**> button.
7. A prompt will come up asking the user which printer is connected to the unit. Choose "**PENTAX**".

   NOTE: Once a printer is chosen, the user will not be prompted again until the unit is rebooted.

8. Follow the instructions on the screen. A report should now print.

   NOTE: If you cannot determine the "shiny" side of the thermal paper from sight, drag your fingernail along both sides of the paper. It will leave a groove on the "shiny" side.

Every operation performed with the Talon® also writes a copy of the report to the CF Drive. This report can be easily accessed in Windows and printed from a text editor like Notepad.

Printing with a Standard (non-thermal) Printer

The Talon® is capable of printing to any ASCII printer. To do so:

1. Connect the printer to the Forensic Talon® using a parallel cable that is compatible with the printer.
2. Power the printer using the printer power adapter.

   CAUTION: Don't confuse this power adapter with the Forensic Talon® power adapter. Press the power button on the printer until it lights up

3. Load plain paper into the printer. The printer will engage and advance the paper slightly.
4. On the Forensic Talon®, press the <**Set**> button to go to the Settings menu. Scroll down to the Printer option and press the <**Select**> button
5. Scroll to the "Select reports…" item and press the <**Select**> button.
6. Scroll to the "Print Last Session" item and press the <**Select**> button.
7. A prompt will come up asking the user which printer is connected to the unit. Choose "**STANDARD**".

   NOTE: Once a printer is chosen, the user will not be prompted again until the unit is rebooted.
8. Follow the instructions on the screen. A report should now print.

Every operation performed with the Talon® also writes a copy of the report to the CF Drive. This report can be easily accessed in Windows and printed from a text editor like Notepad.

Optional Preference Settings

Verify

The Verify option is provided to add an increased level of confidence in the capture process. The choices are: SHA-256, SHA-256 + V, MD5, MD5 + V and None.

SHA-256 - This is the default setting for verification and uses special hardware to compute SHA-256 values at an extremely fast and accurate rate.

SHA-256 + V- This setting behaves like SHA-256, except that it also reads back captured data and compares it to the Source drive. This setting is recommended to ensure the accuracy of the SHA-256 Hash.

MD5 - This setting uses special hardware to compute 128-bit MD5 values at an extremely fast and accurate rate.

MD5 + V- This setting behaves like MD5, except that it also reads back captured data and compares it to the Source drive. This setting is recommended to ensure the accuracy of the MD5 Hash.

NOTE: The "+ V" settings will double the cloning time of a capture session.

None- No verification. This setting is only recommended for non-Forensic cloning operations.

NOTE: Without verification, bad or weak sectors on the Destination drive will not be detected. This could cause the copy to be invalid.

Speed

The speed setting provides the option to set the speed at which an operation will be performed at.

UDMA-5 - The software performs a test procedure to determine the fastest setting that the drives will tolerate while streaming data from one to the other. When set to UDMA-5, all speeds grades below will be tested (i.e. UDMA0-5, PIO0-4)

UDMA-4 - Force the unit to use at most this speed. Set the unit to this mode in some rare situations where one or both drives do not support the higher speeds, and "misbehave" during our automatic speed benchmarking.

UDMA-3 - Same as **UDMA-4.**

UDMA-2 - Same as **UDMA-4.**

UDMA-1 - Same as **UDMA-4.**

UDMA-0 - Same as **UDMA-4.**

PIO-Auto (PIO-4) – Force the unit to use this as the highest speed (PIO-4). Set the unit to this mode in some rare situations where one or both drives do not support higher speeds, and "misbehave" during our automatic speed benchmarking.

PIO-Medium – This is a fixed value that almost all drives will tolerate. It will result in copying speeds from about 200 to over 500 MB per minute depending upon the characteristics of the drives.

PIO-Slow – This is a speed value that all drives will be able to tolerate. It supports copying

speeds from 100 to over 300 MB per minute depending on the characteristics of the drives.

NOTE: Use the MEDIUM or SLOW modes if you encounter drive “time-outs” or if you are capturing older drives. Many older 2.5” notebook drives require the PIO-SLOW setting.

On Error

The On Error setting determines the behavior of the unit in the case where bad spots are detected on the source (suspect) drive. This setting has four options, which include:

Skip - This is the default setting. Skip will allow the Forensic Talon® to continue by stepping over the bad sector.

Abort - This mode will cause the Forensic Talon® to halt if an error such as a bad suspect drive sector is encountered.

Retry - Retry will instruct the Forensic Talon® to make several attempts to read data from the damaged area of the drive.

Recover - Recover will attempt to recover as many bytes of data as possible from each bad sector that is encountered

NOTE: Data in any skipped sectors will NOT be copied to the destination drive. The corresponding sector of the Destination drive will instead be “padded” with zeroes. The padded sector will then be included in the Final SHA-256 or MD5 Value.

NOTE: The absolute location of each skipped sector will also be listed on the final Capture Report. The first 200 bad sectors will be recorded, after which the unit will continue to skip bad sectors but it will not record their absolute locations. The final capture report will show the total number of sectors skipped.

Table 1. Error settings

Option	Action	Time to complete
Abort	A bad sector aborts the cloning operation	Immediate
Skip (default)	Skips the bad sector	Fast
Retry	Attempts several retries to recover data of sector, then skips	Slower
Recover	Attempts a full-blown recovery algorithm, then skips	Very slow

Note: When capturing a Source drive that is known to have many bad sectors, the speed should be set to PIO-AUTO. Also, if the drive is captured or scanned multiple times, the SHA-256/MD5 Hash value of each session could differ. This is because some bad sectors will read intermittently.

Capturing Data from HPA and DCO Configurations

Some PC manufacturers will employ a utility that creates a HPA or DCO configuration on a hard drive. These configurations are designed to change drive characteristics such as drive capacity, speed and other settings as they are reported to the PC BIOS.

HPA – Or Host Protected Area can limit the size of a hard drive, but it can also change many other settings such as speed and S.M.A.R.T. status.

DCO – Or Device Configuration Overlay limits the size of a drive only. For example, a 60GB drive can be made to look like a 30GB drive to a PC.

The Logicube Talon is able to unlock and capture data from a HPA. Furthermore, an Talon® running software version 2.38 or later can unlock and capture data from a DCO. It will then re-lock the DCO. HPA's are relocked when the Source drive is hard-booted after capture.

The Final capture report is also able to report any HPA and/or DCO that is found.

The report only shows the existence of an HPA and if it was unlocked. It looks like this:

```
*------------------------------------------------------------------------------------------ *
*                      SESSION SETTINGS                                                     *
*------------------------------------------------------------------------------------------ *
* Operating Mode: Capture          Address Mode: LBA                                        *
* Verify       : HW-MD5            Speed   : UDMA-4                                         *
* Connection   : Direct                                                                     *
*                                                                                           *
*   100% MIRROR COPY COMPLETED, HOST PROTECTED AREA WAS UNLOCKED!                           *
```

The report also shows the existence of a DCO and if it was unlocked and captured. It also lists the maximum LBA, size and speed setting of the DCO

The report looks something like this:

```
*-------------------------------------------------------------------------------------------*
*                                  SESSION SETTINGS                                         *
*-------------------------------------------------------------------------------------------*
* Operating Mode: Capture              Address Mode: LBA                                    *
* Verify       : MD5                   Speed   : UDMA-4                                     *
* Connection   : Direct                                                                     *
*                                                                                           *
*     100 % MIRROR COPY COMPLETED, DCO WAS UNLOCKED & CAPTURED!                             *
*     DCO ON SOURCE: Maximum LBA:78000000; Size:124999; Speed:UDMA6                         *
*                                                                                           *
*   Operator declined FULL and remainder Destination Drive erase!                           *
*****************************************************************************************
**************************     SOURCE DRIVE     **************************
*****************************************************************************************
*-------------------------------------------------------------------------------------------*
*                                  Physical Characteristics                                 *
*-------------------------------------------------------------------------------------------*
* Drive Model: WDC WD400BD-75LRA0                                                           *
*     Serial: WD-WMAMC4980088                                                               *
*                                                                                           *
*   Cylinders    Heads    Sectors     Total Sectors     Drive Size                          *
*     77504        16       63         78125000         37.3 GB                            *
*                                                                                           *
```

HPA and DCO configurations can only be detected on the Source drive. They cannot be seen on the Destination drive. The following Modes are able to detect, unlock and work with data inside HPA and DCO configurations when the drive is in the Source position:

- Drive Info
- (Native) Capture
- DD Image Capture (all sizes)
- Drive Defect Scan
- Calc. MD5
- Keyword Search

4. Other Modes

Introduction

This chapter discusses other modes that are found in the Mode Setting menu. They are **Drive Defect Scan**, **Wipeclean™ Destination** and **HASH Scan**.

NOTE: **Keyword Search** is discussed in **Chapter 5** and **USB Drive Mode** is discussed in **Chapter 6**.

Modes

Drive Defect Scan

This function performs a surface scan of the drive media using the drive controller to verify the media. It is designed to look for bad sectors, weak sectors or weak spots, which it reports at the end of the scan.

Procedure

1. From anywhere in the menu system press the <Set> button to enter the Settings menu.
2. Scroll to the top item called “Mode” and press the <Select> button. The Mode screen appears.
3. Scroll to “Drive Defect Scan” and press <Select> again.
4. Scroll down to the “Drives” setting. Choose the Source or Destination drive to scan.
5. Scroll down to the “Speed” setting. Here you have two choices:
   - **FAST**: This mode does a single surface scan of the drive. None of the data is moved around or removed.

- **THOROUGH**: This mode actually writes patterns to the drive and scans more thoroughly for bad sectors.

NOTE: Never perform a Thorough Scan on a Suspect drive as data erasure will result.

6. Press the **START**/**STOP** button to start the scan.
7. The Talon® will access the CF Drive, then the following message will appear: "KEYPAD ENTRY: Enter Log file name. Press Select when done".
8. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Select button when finished.
9. When finished, the Talon® will display the number of bad or weak sectors found on the drive. A copy of the session report will also be copied to the CF drive as <Log file name>.LOG.
10. If the Printer was set to "Yes", the user will be prompted to connect the printer and make sure that it is powered up and online. Press SELECT to print or BACK to skip printing.

NOTE: Please refer to "*Printing a Report*" on page 20 for more printing options.

WipeClean™ Destination

This function is the process that erases or wipes all existing information from the surface of the Destination drive. It is a good idea to erase the drive prior to performing Native captures. It ensures that no old data remains on the drive, to be later confused as evidence.

Many newer drives will also support **Security Erase Mode**, which is a much more automated process for wiping data. This mode sends "Security AT" commands to the Destination drive, which allows it to wipe at a very high rate of speed. It also eliminates the need for a Source drive to copy the original pattern from. The unit will automatically switch to Security Erase if it is supported by the attached drives.

NOTE: Security Erase will not run as part of a Native Capture session. Ordinary WipeClean mode is used instead.

Procedure

1. From anywhere in the menu system press the <Set> button to enter the Settings menu.
2. Scroll to the top item called “Mode” and press the <Select> button. The Mode screen appears.
3. Scroll to “**Wipeclean Dest.**” and press <Select> again.
4. Set the Speed and Printer settings, if necessary.
5. Set the Signature setting to the desired position, there are two choices:
   - **YES** (Default): Writes a small signature to the drive every 16.065 sectors (or every logical cylinder). During a later capture session, this signature tells the Talon® that the drive has been correctly erased.
   - **NO**: Leaves the signature off the drive. The Talon® will not detect that the drive has been erased.
6. Press the <Start/Stop> button to begin wiping.
7. The Talon® will access the CF Drive, then the following message will appear: “KEYPAD ENTRY: Enter Log file name. Press Select when done”.
8. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Select button when finished.
9. The Talon will automatically detect whether or not the Destination drive will support a Security Erase. If not, then the Talon will perform an ordinary WipeClean operation based on the settings chosen by the user.
10. If the Talon performs a Security Erase, it will do a rough estimate of the Time Remaining. This estimate will appear on the progress bar while an “Elapsed Time” counter will count up the actual erase time.

    NOTE: The Progress bar will appear to “hang” at 99% if the actual erase time is longer than the estimated time. The elapsed time counter will continue to run and the Status light will keep blinking until the wipe is finished.
11. When finished, the Talon® will display the following message “drive successfully erased”. A copy of the session report will also be copied to the CF drive as <Log file name>.LOG.

NOTE: The operation will abort with an error message if bad sectors are encountered on the Destination drive.

12. If the Printer was set to “Yes”, the user will be prompted to connect the printer and make sure that it is powered up and online. Press SELECT to print or BACK to skip printing.

NOTE: Please refer to “*Printing a Report*” on page 20 for more printing options.

HASH Scan

This mode computes the SHA-256 or MD5 Hash value for a given drive (Source or Destination). It can also scan individual files (on the Destination Drive).

When using this mode, hard drives attached to the Source position (outside) will hash at PIO-AUTO speeds. Hard drives attached to the Destination position (inside) will hash at UDMA-4 speeds.

Procedure

1. From anywhere in the menu system press the <Set> button to enter the Settings menu.
2. Scroll to the top item called “Mode” and press the <Select> button. The Mode screen appears.
3. Scroll to “Calc HASH” and press <Select> again.
4. Set the Speed and Printer settings, if necessary.
5. Set the Method setting to “SHA-256” or “MD5”.
6. Set the Drive setting to scan the Source drive, Destination Drive or a single file.
7. If a certain number of sectors need to be scanned, go to the “Size” setting. Press the <SELECT> button. You can then use the <ARROW> and <SELECT> keys to choose the correct size of the drive.
8. Press the <START/STOP> button to begin the scan.
9. The Talon® will access the CF Drive, then the following message will appear: “KEYPAD ENTRY: Enter Log file name. Press Select when done”.

10. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Select button when finished.

    NOTE: The operation will abort with an error if bad sectors are found on the drive.

11. When finished, the Talon® will display the SHA-256 or MD5 Hash value. A copy of the session report will also be copied to the CF drive as <Log file name>.LOG.

12. If the Printer was set to "Yes", the user will be prompted to connect the printer and make sure that it is powered up and online. Press SELECT to print or BACK to skip printing.

    NOTE: Please refer to "*Printing a Report*" on page 20 for more printing options.

Audit Trail

This mode is used to verify the authenticity of a session report that has been written to the CF Drive. It is designed to check for report alteration. It verifies a proprietary Hash value that was written to the end of the report at the time of creation.

Procedure

1. From anywhere in the menu system press the <Set> button to enter the Settings menu.
2. Scroll to the top item called "Mode" and press the <Select> button. The Mode screen appears.
3. Scroll to "Audit Trail" and press <Select> again.
4. The TALON unit will initialize the CF Drive briefly. After that it will display a list of the Log files that are on the CF Drive.
5. Scroll to the desired Log file and press Select.
6. If the report has not been altered, the message will read "Log file authenticated. Press any key to return".
7. If the report has been altered in any way, the message will read "Log File not authenticated. Press any key to return".
8. Press a key to return to the Main Screen.

5. Using the CloneCard Pro™

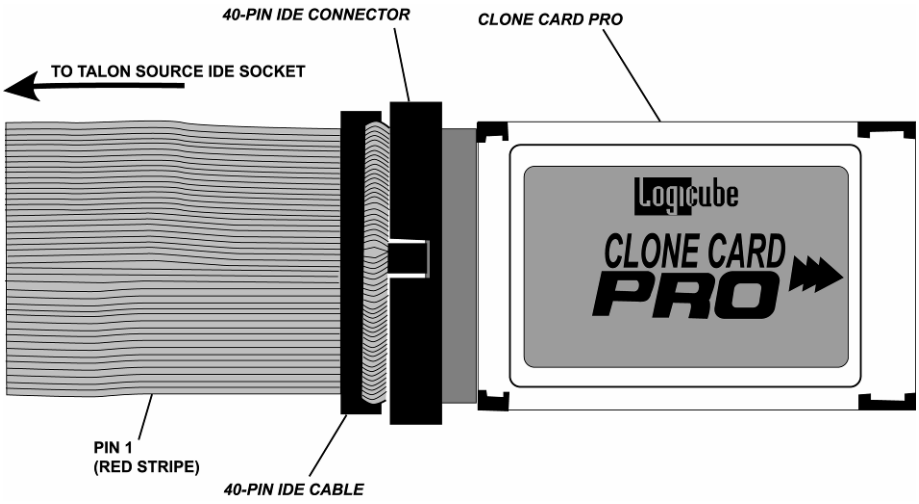
Introduction

The CloneCard Pro™ is an intelligent PCMCIA adapter designed to provide fast cloning to and from laptop PC's. When used properly, it will support up to 175 MB/min transfer speed.

The CloneCard Pro™ is a real time-saver when a laptop drive needs to be captured, and it is undesirable to remove the internal hard drive from the PC. It is designed to work in both PCMCIA (16-bit) and CARDBUS (32-bit) systems.

In general, the user would boot the laptop from the supplied floppy and run a client program. This client program detects the PCMCIA chip-set inside the laptop and will enable communication to the CloneCard Pro™. Now the Forensic Talon® can be connected to the external cable of the card, and operation commences as if the Forensic Talon® is connected to a `real' Source (suspect) hard drive. All Forensic Talon® modes and options are operational as though an actual drive is connected, with the exception of the speed of transfer.

Figure 5. Clone Card Pro™



Before Capturing

Logicube provides a client floppy disk. The floppy has the FREEDOS operating system. In some cases it may be desirable from a compatibility point of view to install a `real' MS-DOS operating system onto the supplied floppy. This can be done on a WIN9X or a DOS machine.

Creating a MS-DOS floppy boot disk

1. Open a DOS window or boot a PC in DOS mode.
2. Unprotect the client floppy disk and insert into the A: drive.
3. At the command prompt (e.g. c:\>) type**: sys a**: <ENTER>.
4. Wait for completion.
5. Copy **Himem.sys** from C:\Windows to the floppy.

Note: This operation needs to be done just once, but cannot be carried out on an NT, WIN2000, XP, or a Windows ME system.

Using the Logicube CloneCard™ Pro to Capture a Drive

Cloning with the CloneCard™ takes just a few steps.

1. Insert the CloneCard Pro™ into one of the PCMCIA slots on the laptop you are about to clone (make sure to remove all other PCMCIA cards.
2. Insert the floppy into the laptop floppy drive
3. Turn laptop on. Ensure that the laptop is set to boot from a floppy. This is done through the setup screens that can be accessed by pressing F2 or <DEL> key during initial boot (consult your laptop manual regarding how to set the boot order).
4. The floppy is configured to run the client application (CCclient.exe or pcmcia.exe) automatically.
5. Connect the Forensic Talon® to the flat cable provided with the CloneCard Pro™. **Do not use the standard drive cable. It is incompatible with the CloneCard Pro™!**
6. Make all the necessary settings on your Forensic Talon®.

7. Set the Forensic Talon® to PIO-Medium speed**.** No settings are available on the client program.
8. Press the **START/STOP** button and wait for the process to complete.

Things to note

1. To verify proper communications with the laptop without starting a Capturing session, try to get Source drive information by pressing the <Drives> button, then the <Source> button from the main screen. You should see the details of the laptop drive. Speed and seek time are likely to be zero, since these benchmarks are not run on the CloneCard. All other information (e.g. drive model, make, size in sectors, etc.) should display properly.
2. If a CD-ROM is available, you can create a bootable CD-ROM that includes *pcmcia.exe*. Make sure your CMOS settings allow booting from a CD-ROM.

   NOTE: Please contact Logicube Technical Support if you need help with creating a bootable CD-ROM.
3. Laptops that have no floppy or CD-ROM drives will require more effort in order to work.

   A. If a docking station is available, use it to boot to DOS.

   B. If the floppy or CD-ROM drive connects through the PCMCIA slot, and only one slot is present as on many palmtop computers (e.g. some Sony VAIO models), follow these steps to boot properly.

      - Prepare a bootable floppy (or CD-ROM) that creates a RAMDISK in memory, then copies ccclient.exe onto the RAMDISK and executes it. (Please contact Logicube's technical support at *techsupport@.logicube.com* for help).
      - Remove the floppy drive with the PCMCIA card
      - Insert the CloneCard™.
      - Perform the cloning session
      - Reboot the laptop.

C. Other laptops require a USB floppy drive to boot.

Improving Speed of Transfer

Several settings in the CMOS setup screens can potentially improve the speed of transfer.

1. **PCI latency timer** - Try to reduce the value of this number as much as possible.
2. **PCI write buffer** - Set to enable to improve writing speed to the local drive.
3. **PCI zero-wait states** - Enable to decrease PCI cycle time.
4. **PCI delay transaction -** Disable to decrease PCI cycle time.
5. **PCI dynamic bursting** - Set to yes.
6. **Enable 32-bit access to hard drive -** We test for that, and if available, we use it to improve transfer speed, so no action is required on behalf of the user.

   NOTE: Some of these settings may not be present on your machine. Also, some of these settings may cause other peripherals to not function properly, so use with caution, and always change one setting at a time.

Supported chip-sets

Below is a partial list of supported chip-set manufacturers:

- Ricoh
- Texas Instruments
- Sony
- Databook
- Vadem
- Cirrus logic Intel
- Toshiba

6. Using the USB Port

Introduction

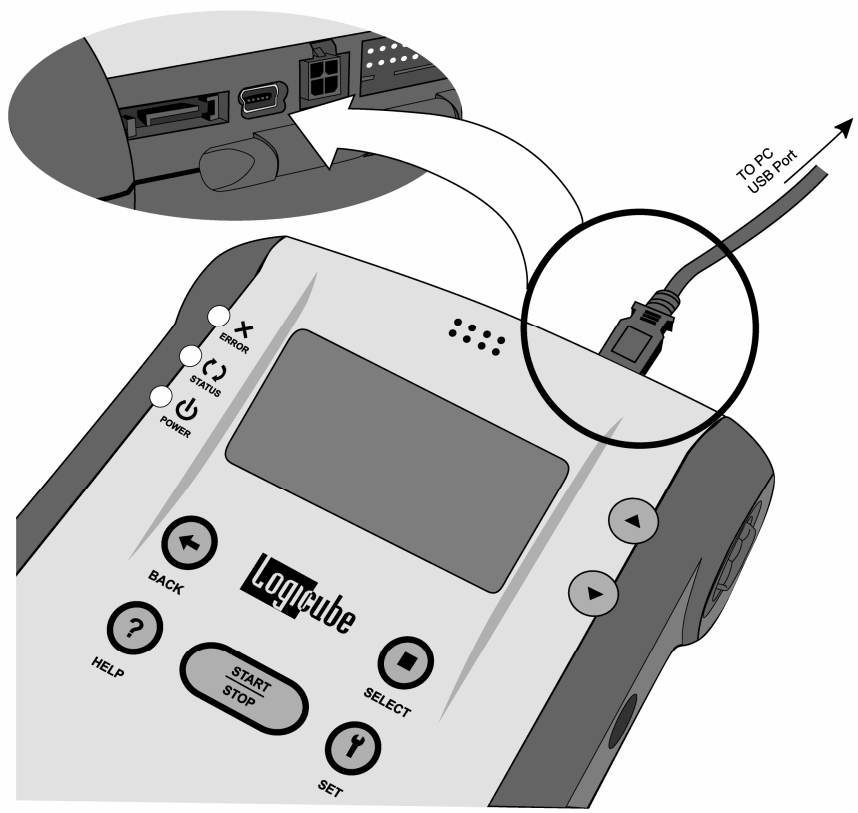
The integral USB port on your Logicube Talon® provides connectivity of your destination hard drive (the unit's internal drive) to any USB-enabled PC. It also ensures zero alteration to the drive under any operating system. Both USB 1.1 and USB 2.0 are supported.

USB connectivity can be used in two modes of operation: Drive analysis mode and DOS capturing mode.

Minimum requirements

- A Logicube Talon® unit with integral USB port.
- A 586 or better PC compatible computer with a floppy or CD-ROM drive.
- An available USB port on the PC. USB 1.1 and USB 2.0 are automatically supported.
- Microsoft Windows 98/98SE/ME/2000/XP operating system (for drive access under Windows).
- A CD-ROM for DOS capturing mode, (optional).
- A CD-ROM with Windows 98/98SE USB drivers installed. No drivers need to be installed for ME/2000/XP.

Figure 8. USB Port on Logicube Talon®



How to use under Windows (for Destination Drive Management)

Please refer to Figure 8 above:

1. Make sure a Destination drive is properly attached inside your Logicube Talon®.
2. Make sure your PC is running Win98 or above.
3. Connect the USB cable (provided) to a PC USB slot on one end. Do not attach the other end to the Logicube Talon® yet.
4. Set the Logicube Talon® to USB mode:
5. Press the SET button on the unit.
6. Scroll up to the MODE: entry. Press SELECT.
7. Scroll down to the USB DRIVE MODE entry. Press SELECT again.
8. Press the Back button to choose “<ATA>”; the unit will access the Master drive. If “<CF>” is chosen, the unit will access the Compact Flash Drive instead.

9. A prompt will come up asking if the unit is connected to a Forensic Dock[1]. Choose **YES** if it is connected to one, otherwise choose **NO**.

   NOTE: Please refer to the Logicube Portable Forensic Lab User Manual if one is in use.

10. The Logicube Talon® will power up the Master drive. A prompt will appear saying that it is safe to attach the USB Cable.
11. Attach the USB cable to the Logicube Talon®. You should now see some activity on your PC screen, which depends on the operating system.
12. If running ME/2000/XP your drive will automatically be mounted and drive letters assigned to all recognizable partitions.
13. If running 98/98SE you will be prompted to install drivers. At the “have disk…” prompt please point the PC to the drivers CD-ROM (provided), and the installation should complete smoothly.
14. The Master Drive is now visible on Windows as an external drive. Any partitions that can be accessed by your Operating System will be assigned a Drive Letter.

At this point the drive is fully visible to any Forensic analysis tool, such as EnCase, iLook, and FTK. The drive contents, however, cannot be altered in any way. Note that since Windows keeps caching information for every drive, some operations (such as file read), may appear to show changes in file access time etc. but these are purely virtual, and do not change anything on the drive itself.

Removing USB devices

Before physically disconnecting the USB cloning adapter and/or shutting down power to the Logicube Talon®, the unit has to be properly "unmounted" from Windows. To do that:

1. Locate the USB icon in the system tray (typically at the bottom right of screen).

2. Click the icon once.

[1] The Forensic Dock refers to the Portable Forensic Lab, which is a Logicube product that is sold separately.

3. Wait for Windows to bring up a message that it is safe to remove the device. (Different versions of windows will behave slightly differently).

Cloning through the USB port

This mode allows the user to clone drives through the USB port of a PC. The PC drive can only be the Source drive. Both USB 1.x and 2.0 are supported. Typically, the user will boot the computer from the provided boot CD. The CD is equipped with USB drivers and our drive capturing application.

How to set up and use the USB Cloning software:

1. Follow these instructions to maintain the forensic integrity of the capture. With computer power off, insert the boot CD into the CD-ROM drive or, depending on the computer's CD-ROM drive you may need to insert the CD as far as it will go so it can be pulled in during power up. Start the computer and immediately enter the BIOS setup menu. This varies by computer but usually requires you to press (F12, F1 for IBM or the Delete key for most generic PCs) just after startup. Make sure that the PC is set to boot from the CD-ROM as the first bootable device. Allow the PC to continue booting off of the boot CD in the CD-ROM drive.
2. The Forensic USB Cloning CD-ROM is configured to automatically load the necessary drivers and run the client application. The user will be presented with a User Interface and a menu to select among the various capture options and settings.

NOTE: A USB connection must be made between the computer and the Logicube forensic capture device either before or after the Boot CD application starts. The following message will be displayed if the application starts without detecting a connection to the Logicube forensic capture device: *Searching for Logicube Forensic Device. Make sure it is connected.*

3. On the Logicube Talon® attach a hard drive to the Destination (Internal) position that is larger than the suspect drive you intend to capture.
4. Attach a USB cable to the PC (do not attach the other end of the cable to the Logicube Talon® yet).
5. Engage the Talon in USB mode as described in the procedure listed under “Master Drive Management”, (follow steps 5 – 10).
6. Attach the USB cable to the Talon. The PC client software should now detect the presence of the Logicube Forensic Talon you are using. The cloning software interface will then come up. All available functions will now be controlled from the PC client software application. The application will display a menu containing three columns *PC Source Drives, Partitions and Modes.*

NOTE: For DD captures only, if the destination drive is not formatted with a FAT32 partition, the application will prompt the user and will format the drive accordingly. If there is not enough room in the destination drive for a DD file capture, the application will exit with an error, notifying the user.

Selectable Capture Modes & Options

- **Native:** This is analogous to a mirror copy of the PC’s internal drive to the Destination. This mode calculates and displays an MD5 Hash value.

- **Native +V:** Capture suspect drive and compute MD5 on the master drive. The destination drive is then read back, an MD5 hash is computed on it and compared with the Master hash. The Capture Utility display the Total MD5 Hash value on the screen at the end of the capture session.

- **DD-Image-650M:** The Master drive is broken up into (650 M byte files) and a MD5 hash is computed on every file. (MD5 Hash values are calculated for each DD image) This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.

- **DD-Image-650M+V:** The Master drive is broken up into (650 M byte files) and a MD5 hash is computed on every file. The destination drive is

then read back, an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.

- **DD-Image-2G:** The Master drive is broken up into (2 G byte files) and a MD5 hash is computed on every file. This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.

DD-Image-2G+V: The Master drive is broken up into (2 G byte files) and a MD5 hash is computed on every file. The destination drive is then read back, an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.

- **DD-Image-4G:** The Master drive is broken up into (4 G byte files) and a MD5 hash is computed on every file. This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.

- **DD-Image-4G+V**: The Master drive is broken up into (4 G byte files) and a MD5 hash is computed on every file. The destination drive is then read back, an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.

- **Compute Source MD5:** An MD5 hash is computed on the entire internal PC drive. The resulting value is displayed on the screen.

- **Compute Destination MD5:** An MD5 hash is computed on the entire destination drive. The resulting value is displayed on the screen.

- **Erase Destination:** A single pass wipe is performed on the destination drive. For erase the Capture Utility reports Total Drive Sectors, Erased Sectors, Erase speed in MB/Minute, Time to Completion and % Complete.

7. Use the arrow keys on your host PC's keyboard to navigate through the various settings of the

capture utility. Use the “Enter” key to make selections and the “S” key to start a process.

8. On the left side of the screen you will see a list of up to four available drives. Choose the “Source” drive you wish to capture by scrolling through the selections using the up/down arrow keys on your PC’s keyboard. When your selection is highlighted a brief description of the drive will appear in the middle of the screen. Press “enter” to select a source drive.
9. On the right side of the screen you will see a list of capture modes. You can scroll through the selections using the up/down arrow keys on your PC’s keyboard. Press “enter” to make your selection.
10. Once you have selected the “source” drive to be captured and selected the method of capture press “S” to start the data capture. A progress bar will appear on the screen.
11. You may cancel or abort the capture at any time by pressing the “Esc” key. Press any key and answer [Y]es to return to the main menu.
12. Once the capture has been completed a message will pop-up indicating the capture session has completed successfully.
13. If you have selected a capture method with an MD5 Hash, the hash values will appear at the bottom of the screen**.**

NOTE: Except for DD captures, the hash values generated will not be saved if you exit this screen. You must record the hash values before exiting!

14. Upon completion of the data capture press any key and answer [Y]es to go back to the main screen. To perform a data capture from another source drive, install a new destination drive only if the current destination drive is full or your next capture will be performed as Native. Repeat steps 7 through 14 to perform a subsequent data capture.
15. To exit the Forensic Cloning Software, press the Esc key and answer [Y]es. A message will display that indicates “You can now remove the CD-ROM”. Some computers will automatically eject the CD at this point. Power down the PC as soon as the CD has been removed from the CD-ROM drive to maintain the forensic integrity of the capture. *Do not re-boot!*

Cloning Apple computers via FireWire using the USB Cloning software:

1. Follow these instructions to maintain the forensic integrity of a HDD capture from an Apple computer. Ensure that the Apple computer is turned OFF.
2. Install a FireWire cable between the host PC running the cloning software and the Apple computer to be cloned.
3. Power up the Apple computer, wait for the BIOS chime and immediately press and hold "T" to enter FireWire Target Disk Mode.
4. With FireWire Target Disk Mode already established, the User Interface on the analysis PC will display the Apple computers hard drive in the list of available drives as soon as the cloning software is loaded.
5. Load the cloning software CD onto the non Apple PC by following instructions 1 - 15 above.

Additional Notes

- To clone a drive associated with an Apple PC the analysis PC running off of the boot CD must have both FireWire and USB ports.

- Capture speed depends wholly on the USB and FireWire hardware and the processor speed of the PC. Expected capture speeds are up to 1.4GB/min with verify and up to 1.8GB/min without verify. Your capture speeds may vary.

- 400/200/100 speed FireWire ports are supported. 800 Mbps FireWire is not supported.

- Upon detection of an error the capture will skip the bad sector(s) and write zeroes to the corresponding sector(s) on the destination drive.

- Older computers may require the use of a bent paper clip to eject the drive tray for boot CD installation and removal.

- During most operations the capture utility reports Total Drive Sectors Cloned, Speed in MB/Minute, Time to Completion and % Complete.

- Due to the absence of a Firewire connection MacBook Air is not compatible with the Logicube boot CD.

7. Using the RAID I/O Adapter

Introduction

The Logicube RAID I/O Adapter™ is designed to work exclusively with the Talon®. It is an adapter that allows two hard drives to be connected to the Source or Destination position simultaneously.

In the Destination Position, or “RAID 1-to-2”, the RAID I/O Adapter™ allows two Destination drives to be cloned at the same time. This is important if the investigator needs to have one drive for evidence and a second drive for investigation.

In the Source position, or “RAID 2-to-1”, the RAID I/O Adapter™ will allow two drives in a RAID-0, RAID-1 or JBOD configuration to be cloned to a single Destination drive. This feature is only supported with a software option that needs to be loaded on the Talon™.

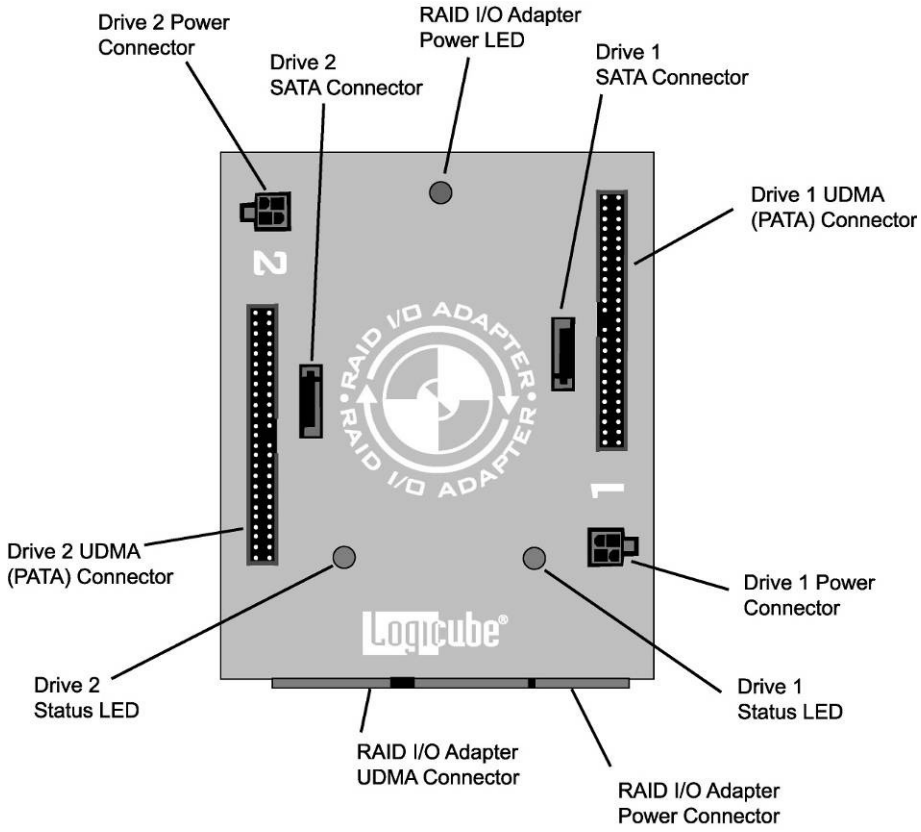
NOTE: The Talon® must have software ver. 2.36 or later installed in order to properly work with the RAID I/O Adapter™.

NOTE: Please refer to Chapter 10 – “Enabling the RAID 2-to-1 Option” for the procedure to load the software option on the Logicube Talon®.

Connecting the RAID I/O Adapter

Please refer to Figure 9 below:

Figure 9 – RAID I/O Adapter



NOTE: The following directions pertain only to the RAID I/O Adapter™ as it is used in the Destination Drive position.

Attaching the RAID I/O Adapter™ to the Talon®is very similar to attaching an IDE (PATA) drive:

1. Open the Logicube Talon® by pressing on the two latches at the base of the unit and lifting the top. You will notice three connections: One for a flat cable (the drive data cable) and another for a small drive power cable. Underneath is the third connector for the Serial ATA cable.

   NOTE: Please refer to **Chapter 2 – Getting Started** for more information on connecting hard drives.

2. Connect the Raid I/O Adapter™ to the UDMA (PATA) drive power and data cables. Leave the Logicube Talon® lid open.

3. Connect Destination Drive 1 and 2 to the appropriate connectors on either side of the RAID I/O Adapter.

   Note: A Destination drive can be connected to either position on the RAID I/O Adapter™, if only one Destination drive is to be used.

4. Connect the Source drive to the outside of the Talon® if using the RAID I/O Adapter in a 1-to-2 configuration..

5. Connect the external power supply to the Logicube Talon® and power-up the unit. In 2 – 3 seconds, the main "Splash" screen appears.

Cloning with the RAID I/O Adapter™ in 1-to-2 Mode

Both Native Capture and DD Image Capture Modes work with one or two Destination drives. The procedure for cloning is exactly the same as cloning to a single Destination drive without the RAID I/O Adapter™. Both drives will appear in the final capture report.

Verification Modes, Drive Defect Scan Mode, WipeClean Destination Mode, Calc. MD5/SHA-256 Mode and Keyword Search Mode can only work with one Destination drive attached to the RAID I/O Adapter. The drive can be in either position. If two destination drives are attached, the selected operation will be performed only to the drive attached to position 1.

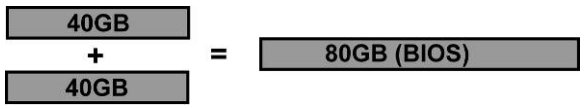
USB Mode is not compatible with the RAID I/O Adapter at this time. This incompatibility also extends to USB cloning.

Cloning with the RAID I/O Adapter™ in 2-to-1 Mode

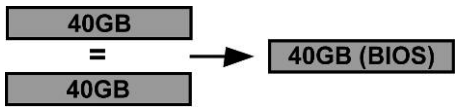
Once the RAID 2-to-1 option is unlocked on the Talon®, The RAID I/O Adapter can clone two RAID drives to a single Destination drive.

Supported RAID Configurations

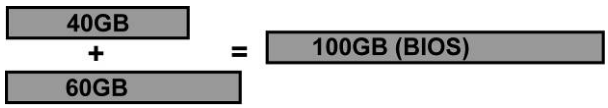
2-to-1 Mode supports **RAID-0**, **RAID-1** and **JBOD** configurations. These configurations are described below:



- **RAID-0:** This configuration splits data evenly over two separate hard drives so that they are seen as one large drive in the PC BIOS. This configuration is also known as a **striped set**.



- **RAID-1:** This configuration creates an exact copy of one drive's data across two separate hard drives. It is designed to provide uninterrupted service should one of the hard drives go down. This configuration is also known as a **mirror**.



- **JBOD:** This configuration is able to distribute data over two drives of different size so that the drives appear in BIOS as one single drive. JBOD stands for **"Just a Bunch of Drives".**

Connecting the RAID I/O Adapter

1. Plug in the set of 9" cables, to the connections found on the back of the Logicube Talon™.

   NOTE: Please refer to **Chapter 2 – Getting Started** for more information on connecting hard drives.

2. Connect the RAID I/O Adapter™ to these cables.
3. Connect Source Drive 1 and 2 to the appropriate connectors on either side of the RAID I/O Adapter.

   Note: A Source drive can be connected to either position on the RAID I/O Adapter™, if only one Source drive is to be used.

4. Connect a single Destination drive to the inside of the Talon™. You cannot use more than one RAID I/O Adapter™ on the Talon® at a time.
5. Connect the external power supply to the Logicube Talon® and power-up the unit. In 2 – 3 seconds, the main "Splash" screen appears.

Cloning with the RAID I/O Adapter™ in 2-to-1 Mode

Drive Info will give information on each Source drive as well as the type of RAID Controller used (i.e. Adaptec, LSI, etc.) and the type of RAID configuration (RAID-0, RAID-1, JBOD). If the configuration is RAID-0, then Drive Info will also show the stripe size (i.e. 128KB). This information will also appear on the final capture report as seen below:

```
*  Drive Model: WDC WD400BD-22JMA0                                    *
*      Serial: WD-WMAM92665729                                        *
*                                                                     *
*   Cylinders    Heads    Sectors     Total Sectors     Drive Size    *
*      77545       16       63          78165360          37.3 GB     *
*                                                                     *
*                 ---   Second Source Drive   ---                   *
*                                                                     *
*  Drive Model: WDC WD400BD-22JMA0                                    *
*      Serial: WD-WMAMC2644889                                        *
*                                                                     *
*   Cylinders    Heads    Sectors     Total Sectors     Drive Size    *
*      77545       16       63          78165360          37.3 GB     *
*                                                                     *
*                      RAID Characteristics                           *
*        RAID Manufacturer: AMCC/3Ware                                *
*              RAID Type: RAID_1                                      *
*  Maximum Virtual Sectors: 78163312                                  *
*        Reserve Sectors(s): 0, 1                                     *
*       Computed MD5 Value: 4701E466 99E1C230 16D8ADC1 DF5DCDA8       *
```

Figure 10 – Final Capture Report with RAID 2-to-1

Both Native Capture and DD Image Capture Modes work with one or two Source drives. The procedure for cloning is exactly the same as cloning from a single Source drive without the RAID I/O Adapter™.

Verification cannot be set to a "+V" setting on the Forensic Talon® or the cloning session will stop with an error message: "The current Verify setting is not supported with a RAID Source". All other verification settings are acceptable and Dual Hash (MD5 or SHA-256) is supported.

Drive Defect Scan is supported for one or two Source drives. The final report will list all bad sectors found on the first drive, then a separate list for the second drive.

Calc. Hash and Keyword Search modes are not supported through the RAID I/O Adapter in the Source position.

Other Notes

To verify the MD5 or SHA-256 Hash with a third party method, RAID Source drives must be write protected, then re-attached to their RAID controller and examined with a software-based utility (like Winhex).

Connecting to different RAID controllers will produce uneven results.

Also, connecting the Source drives without write-protection will change the MD5 or SHA value of the Source drives.

Destination drives can be scanned without the use of a RAID controller.

8. Using the GPStamp™

Introduction

The GPStamp™ provides accurate location, time and date information for a hard drive capture session. This information appears in the final capture report. The GPStamp™ uses GPS (Global Positioning System) technology to provide location coordinates that are accurate to within 50 feet.

The GPStamp™ is designed to work exclusively with the Logicube Forensic Talon® and Forensic MD5™. The GPStamp™ pulls information from four or more GPS satellites to provide the exact capture location in 3D space.

Figure 11 – GPS Satellite

Overview

Please refer to Fig. 12 below.

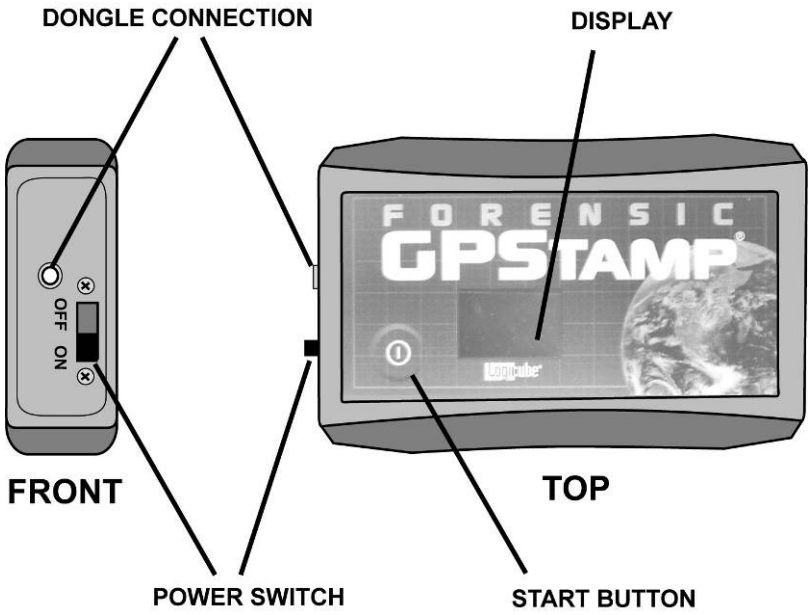


Figure 12. GPStamp Orthographic Views

The GPStamp™ is extremely simple to use with very few user controls:

- **DISPLAY** – This small OLED display is very bright and easy to read.
- **DONGLE CONNECTION** – This jack is where the Adapter cable (Dongle) connects when the GPStamp™ is attached to the Talon® or MD5™.

  NOTE: This jack is NOT a power supply port. The GPStamp™ is powered by an internal 9V Lithium battery.
- **POWER SWITCH** – Turns the GPStamp™ on and off. Keep the switch OFF when the GPStamp™ is not in use.

  NOTE: Although the GPStamp goes into "Sleep Mode", the best way to conserve battery power is to shut the unit off. Sleep Mode still draws a small charge from the battery.
- **START BUTTON** – This button has multiple functions such as starting a location acquisition, "freezing" a reading and bringing the GPStamp™ out of Sleep Mode.

NOTE: The Logicube Talon® must have software ver. 2.37 or later installed in order to use the GPStamp™.

Using the GPStamp™ in a Capture Operation

The following procedure will take you through a typical hard drive capture operation with the Logicube Forensic Talon® and GPStamp™.

1. Attach the Source (Suspect) and Destination (Evidence) drives to the Talon®. Set up all capture settings as desired.
2. In the Settings Menu, scroll down to the "GPS Available" option. Press Select to set it to "Yes".
3. An error message will appear briefly that says, "The GPStamp was not detected". Ignore the message and continue.
4. Start the capture session. After data has been transferred to the Destination drive, the Talon® will display a message that reads "Get Fix".
5. Power up the GPStamp™, when it goes into Sleep mode, press the Start button. The Main Screen will appear.
6. After thirty seconds, the GPStamp™ will attempt to lock on to a signal. The Signal Acquisition screen will appear.
7. The GPStamp™ should acquire a useable signal within two minutes. If it does, then the Information Screen will appear.
8. If the GPStamp™ does not get a signal within five minutes, an error message will appear that reads "Unable to get GPS fix. Take unit to area of good reception. After thirty seconds the unit will try to get a signal for another 5 minutes.

   NOTE: After 60 minutes of searching, the GPStamp™ will go into Sleep Mode if no signal is acquired. Press the Start button to get the unit out of Sleep Mode.
9. When a fix is acquired, press the Start button to "freeze" the information. The unit will begin to count down from five minutes.

   NOTE: Entering an area of no reception with an acquired signal will auotmatically "freeze" the GPStamp™ for five minutes.

10. Attach the GPStamp to the parallel port of the Talon® or MD5™ with the supplied adapter cable. Please refer to Figure 13 below:

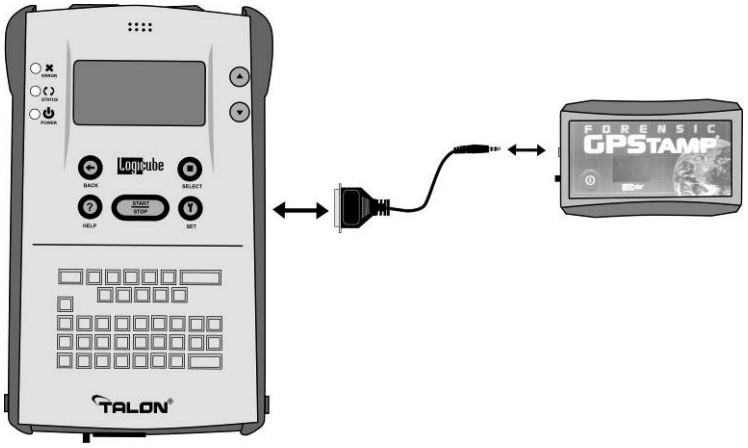


Figure 13. GPStamp™ Connection to Talon™

11. The Talon® or MD5™ will read “Get Fix” as it downloads the information. If it cannot read the GPStamp™ it will read “No Fix”.
12. Once the fix is downloaded to the Talon® or MD5™, it will finish the capture session. The GPS information will appear in the Final Capture Report as shown below:

```
*****     LOGICUBE TALON     Serial No.: 15295  Software: V2.37     *****

 Evidence Number_____________________ Alias_____________________
 Evidence Acquired by_____________________________________________
 Evidence Acquired on_____________________ AT_____________________
  Location/Time          N 34.1412650              W 118.3386953
  0:14:3 UTC             Aug-18-2006               PDOP: 3.13
  Capture To Fix Delay (seconds): 405
 Location at scene________________________________________________

 Description______________________________________________________

                          SESSION SETTINGS

  Operating Mode: Capture          Address Mode: LBA
  Verify        : None                Speed   : UDMA-5
  Connection    : Direct

          100% MIRROR COPY OF THE SUSPECT DRIVE HAS BEEN
           SUCCESSFULLY EXECUTED ON THE EVIDENCE DRIVE!

    Operator declined FULL and remainder Destination Drive erase!
```

Figure 14. Final Capture Report with GPS Information

NOTE: The time and date information are based off of UTC, or Coordinated Universal Time. This time zone is also known as GMT, or Greenwich Mean Time. Hours are displayed in “Military Time” (0 – 23 hours).

9. Keyword searching

Introduction

The Forensic Talon® unit can search for multiple keywords while capturing a suspect drive. This is a useful feature to provide early screening of a drive. For example, one could search for the names of all common drugs or the names of known offenders on a given drive. Presence of these keywords might indicate a connection between the suspect and the words searched for.

In general, the user will select a pre-defined list of words that will be loaded into the hardware based search engine. These words are automatically searched for during the next Capture session. At the end of the session, the user can print one of several reports that indicate the number of occurrences, and absolute location on the drive of all matches found.

All keyword lists are stored on the Compact Flash in a file called keyword1.lst. The file is a simple text file which can be edited by any plain text editor, such as Notepad.

A sample file might look like this:

```
[Terrorism]
ABU NIDAL=case:yes,unicode:no,signature:no
ABU SAYYAF=case:yes,unicode:no,signature:no
AL-QAIDA=case:yes,unicode:no,signature:no
BLACK SEPTEMBER=case:yes,unicode:no,signature:no
DEMORALIZE=case:yes,unicode:no,signature:no
HAMAS=case:yes,unicode:no,signature:no
HIZBALLAH=case:yes,unicode:no,signature:no

[Computer crimes]
2600 =case:yes,unicode:no,signature:no
BACK ORIFICE=case:yes,unicode:no,signature:no
CRACK=case:yes,unicode:no,signature:no
DEFCON=case:yes,unicode:no,signature:no
ENCRYPTION=case:yes,unicode:no,signature:no
FLAME=case:yes,unicode:no,signature:no
HACK =case:yes,unicode:no,signature:no
IP SPOOFING=case:yes,unicode:no,signature:no
```

In the above example, two lists ([Terrorism] and [computer Crimes]), are listed. The user can select only one for each search session. Many more lists with many more words can be defined.

Three options are available for each word:

1. **Case**: - yes/no. If Yes, the word is searched exactly as typed. No, will search for all lower-case, all Upper case, First letter upper-case and exact matches.
2. **Unicode**: yes/no. If No, the plain ASCII of the word will be searched for. Yes, the Unicode encoding of word is searched for.

   NOTE: The Unicode search utilizes the "little endian" code that is utilized by Microsoft operating systems. Other systems, like Linux, UNIX, Mac, etc. utilize the "big endian" code. A future version of the Logicube Talon® software will also support big endian Unicode.
3. **Signature**: the word is only searched at the beginning of sector. This is useful to find all files of a certain type, e.g. all graphic files.

The unit allows some editing of the keyword lists. Please refer to the **Modify Lists** section below for more details.

NOTE: As of this writing, only the English alphabet is supported. Future software updates will include support for different languages. Please contact Logicube for further details.

To search for a pre-defined keyword list during Capture

1. Press the 'Set' button to enter the Settings screen. Set the desired Capture mode and subsequent settings (Speed, Verify, etc.).
2. Scroll down to the 'Word List' option and note the name of the currently selected keyword list. If none is selected, press the 'Select' button.
3. The unit will read the list of available keyword lists from the Compact Flash, and display it on the screen.
4. Scroll to the desired list, and press 'Select'.
5. Form now on, the words in this list will be searched for as a by-product of any of the Capture modes.
6. At the end of a session, the Final Capture report will also list any keywords found. You

can then print one or both Keyword Search reports:

- **Print Search Detail**: This report lists every keyword found and the sector where it resides.
- **Print Search Text**: This report lists every keyword and the surrounding line of text.

NOTE: The DD Image Capture Report will not automatically list keywords. We suggest running the Search Detail report after the Capture Session to list any keywords found.

NOTE: Please refer to "*Printing a Report*" on page 20 for more printing options.

Keyword Search Settings

On Match: This setting determines the behavior of the unit if a Keyword is found. Three settings are available:

- **Log** (Default): This setting writes the Keyword and location to the Compact Flash Card. The file created is called Listfile.txt.
- **Print**: Automatically prints Keyword hits as they are found.
- **Pause**: The unit pauses with a message on the display. This setting is useful to determine if a drive has keywords in the first place.

NOTE: As of this writing, Log is the only setting available. The other settings will be accessible in later versions of the software. Please contact Logicube for availability.

Modify Lists

This menu contains settings that allow you to Add, remove or edit lists from inside the Talon® unit

itself. It is also possible to add keywords to an existing list.

Edit Mode: This mode contains two settings:

Local (Default): Modifies the Keyword Lists on the Compact Flash Drive inserted in the unit.

USB: Grants access to a Keyword List on your PC via the USB port. This setting will be activated in a later software update.

NOTE: The Keyword Lists can also be manipulated on a PC with Notepad or a similar utility. They can be accessed from the Compact Flash Card through a card reader or other device.

Add new list: This setting allows you to add a new Keyword Search List to the Compact Flash Card. When chosen, it first asks you to add a List name. After that, it brings up a screen to add Keywords. Press the START/STOP button once all new words are added.

Edit List: This setting allows Keywords in an existing list to be modified or removed. It also allows new Keywords to be added. When chosen, it asks which list needs to be modified. After that, it brings up a screen with the choice of adding words or modifying existing words.

Remove List: This setting removes a chosen list from the Compact Flash Card.

WARNING: There is no “are you sure” screen once a list is chosen for removal.

Keyword Search Mode

In addition to searching for Keywords during a capture, the Talon® can also perform a separate Keyword Search session. This is done by pressing the ‘Set’ button and changing the Capture Mode to ‘Keyword Search’. All of the settings are identical to those described above. The only addition is the **Drive** setting. This setting allows the Keyword Search to run from the Source or Destination drive.

NOTE: If the Source drive is chosen for a Keyword Search then the speed will drop to PIO-AUTO.

10. Compact Flash (CF) Card

Introduction

The Logicube Talon® comes with a 64MB Compact Flash (CF) Drive that is inserted in a CF slot at the bottom of the unit. This little drive is used mostly for loading software on the Logicube Talon®, storing Keyword Search lists and storing session reports.

NOTE: Please check our website periodically at www.logicube.com, any new CF functions will be posted there.

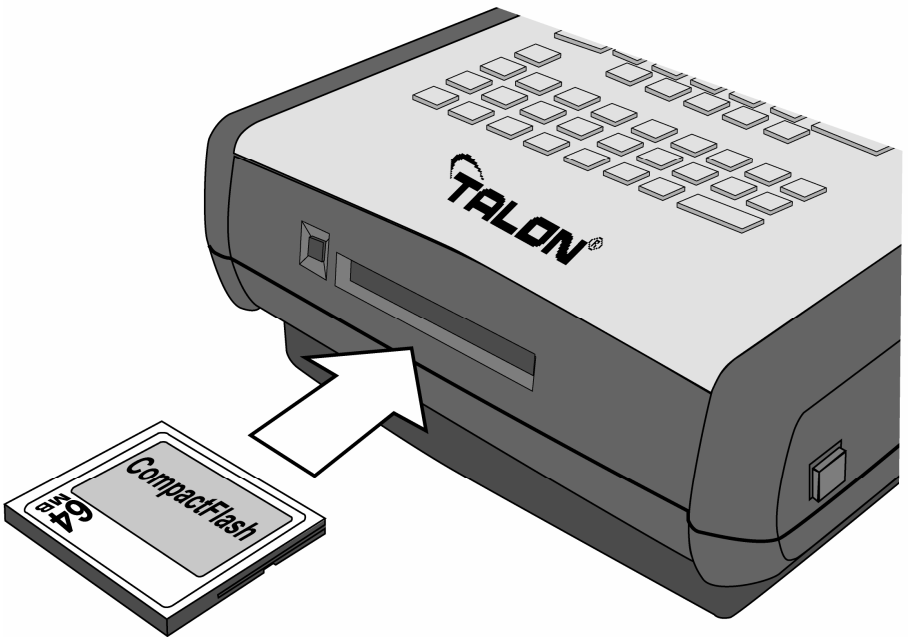
To load new software from the CF Drive, please refer to the procedure "**Loading Software Using the Compact Flash**" which is found in **Chapter 11: Software loading Instructions.**

Inserting and Removing the Compact Flash

Please refer to Figure 10 below.

1. At the bottom of the Logicube Talon® is a Compact Flash (CF) slot. Make sure that it is clear.
2. Hold the CF Drive so that the Logicube label faces up.
3. Slide the CF Drive into the CF slot. As it slides into place, the eject button will slide out.
4. To remove the CF Drive, simply press in the eject button. The drive will slide out.

Figure 15. Compact Flash (CF) Port Detail.



Connecting the CF Drive to Windows via USB

This is necessary to load new software files to the CF Drive. There are two methods to connect the Compact Flash (CF) Drive to Windows through the USB Port. One is via USB Mode and the other is through the Software Setup Menu.

NOTE: Unlike the Destination drive, the CF drive is NOT Write Protected when it is accessed through USB. This is so new files (like software updates, new keywords, etc.) can be written to the CF Drive.

Connecting Through USB Mode

1. Make sure your PC is running in Windows 98 or above.
2. Connect the USB cable (provided) to the USB port on the Talon®, and to a PC USB slot on the other end.
3. Set the Forensic Talon® to USB mode:
4. Press the SET button on the unit.
5. Scroll up to the MODE: entry. Press SELECT.
6. Scroll down to the USB DRIVE MODE entry. Press SELECT again.

7. At the first prompt, press the Select button to choose “<CF>”.
8. A second prompt will come up asking if the unit is connected to a Forensic Dock. Choose **YES** if it is connected to a Portable Forensic Lab, otherwise choose **NO**.

   NOTE: Please refer to the Logicube Portable Forensic Lab User Manual if one is in use.
9. The Forensic Talon® will now power up the CF drive.
10. You should now see some activity on your PC screen, which depends on the operating system.
11. If running ME/2000/XP your drive will automatically be mounted and drive letters assigned to all recognizable partitions.
12. If running 98/98SE you will be prompted to install drivers. At the “have disk..” prompt please point the PC at the drivers CD-ROM (provided), and the installation should complete smoothly.

The CF Drive is now visible on Windows as an external drive. You can copy software update files, or anything else to/from the drive.

Connecting Through the Software Setup Menu

If the software on your Logicube Talon® is corrupt or missing, USB connectivity is still available for the CF drive through the Software Setup Menu. This menu resides in the unit’s Firmware and is not affected by the software.

1. Make sure your PC is running in Windows 98 or above.
2. Connect the USB cable (provided) to a PC USB slot on one end. Do not attach the other end to the Talon® yet.
3. Boot The Logicube Talon® while holding down the START/STOP button. The unit will boot to the Software Setup Menu.
4. Scroll down to “Engage CF to USB”. Press the SELECT button.
5. A prompt will appear saying that it is safe to attach the USB Cable.
6. Attach the USB cable to the Logicube Talon®. You should now see some activity on your PC screen, which depends on the operating system.

7. If running ME/2000/XP your drive will automatically be mounted and a drive letter will be assigned to it.
8. If running 98/98SE you will be prompted to install drivers. At the “have disk…” prompt please point the PC to the drivers CD-ROM (provided), and the installation should complete smoothly.
9. The CF Drive is now visible on Windows as an external drive. You can copy software update files, or anything else to/from the drive.

Removing USB devices

Before physically disconnecting the USB cloning adapter and/or shutting down power to the Logicube Talon®, the unit has to be properly "unmounted" from Windows. To do that:

1. Locate the USB icon in the system tray (typically at the bottom right of screen).

2. Click the icon once.

3. Wait for Windows to bring up a message that it is safe to remove the device. (Different versions of windows will behave slightly differently.

11. Software Loading Instructions

Enabling the RAID 2-to-1 Option

RAID 2-to-1 is an option that allows the Forensic Talon® to interface with the RAID I/O Adapter in "2-to-1" Mode. To use an option like RAID 2-to-1, it first needs to be enabled.

NOTE: Please refer to **Chapter 8 – RAID I/O Adapter** for information on using this product with the Talon®.

To enable an option on the Logicube Talon®, contact Logicube to receive a license key that is unique to your unit. Once you have obtained the license key, follow this procedure to enter it into your Logicube Talon®.

10. From anywhere in the menu system, press the Set button to enter the Settings menu.
11. Scroll to the "Enable Option" menu item and press the Select button.
12. Enter the RAID 2-to-1 activation code you received from Logicube.
13. If all symbols have been entered correctly, the Logicube Talon® will reboot to the main menu.
14. To verify that the option has been activated, select About (press the Back button) from the main menu. You will now see RAID 2-to-1 listed as an installed option.

NOTE: Once the license key is entered, an optional software package is permanently enabled. The key will not need to be entered again, unless the Firmware or the BIOS are changed on the Logicube Talon® itself.

NOTE: Loading new software updates will not disable any unlocked options.

Logicube Talon® Software Updating Procedures

New and improved software will appear from time to time on our web site at www.logicube.com. It is possible to update the operating software in the field by a user.

Two common ways are available:

1. Using the Compact Flash card
2. Using a parallel port connection

NOTE: Logicube provides a CD-ROM that contains a backup copy of the Logicube Talon® software. This software is already loaded on your unit.

Loading Software Using the Compact Flash

The new software (a single file always called forensic.h86) has to be placed on the root directory of the Compact Flash (CF). If a CF reader/writer is available on your computer, forensic.h86 simply needs to be copied to the root directory, possibly overwriting the older version that's already there.

Another file called tlncfldr.h86 also needs to be on the root directory of the Compact Flash Card.

NOTE: If a reader is not present, the Logicube Talon® itself can be configured to behave like a CF reader/writer. Please refer to "**Connecting Through the Software Setup Menu**" in **Chapter 10: Compact Flash (CF) Drive**.

Once the new forensic.h86 file is present on the CF, it is a simple matter to make it "re-flash" the unit:

1. Power up the unit while holding down the Start/Stop button.
2. Select the first option "Load SW from CF", and press the Select button. The status light should start to blink.
3. After about 30-40 seconds the unit will re-boot to the new software.
4. Check the version and date of this software by pressing the "About" button at the main menu screen.

Loading Software Through the Parallel Port

This is a legacy method to load software, and should only be used in situations where the CF method cannot be used.

To successfully load new software on to the Logicube Talon® with the parallel port connection, you need the following:

- The Software Update CD that came with your unit.
- A DB-25 Straight-through parallel cable.
- (If loading new software), a floppy or other removable drive with the new version of forensic.h86 loaded on it.
- A host PC with the following:
  - An EPP 1.9 capable parallel port.
  - A CD-ROM drive.
  - A floppy drive or other removable drive accessible by DOS.
  - Ability to boot from a CD. This can be determined by checking the PC's BIOS.

Host PC preparation

1. Place the Software Update CD in the Host PC's CD-ROM drive.
2. Boot the PC and go into BIOS. Make sure that the PC is set to boot from the CD-ROM.
3. Reboot the PC. It will go into a menu on the CD that contains six different boot methods.
4. Try the first boot method. If it doesn't work, reboot and try the second. Keep trying until you find one that works (goes to an A prompt).

Once the above has been accomplished, perform the following:

5. Attach the parallel cable between the host PC and Logicube Talon®.
6. If you are loading a new version of software, Insert the removable drive with the new forensic.h86 file and copy it to the Ramdrive created by the CD.

NOTE: Ignore step 2 if you are reloading the original forensic.h86 file, which is automatically copied to the Ramdrive.

5. Go to the Ramdrive (always the last drive letter) and run **UPDATE**. The Software Update screen will appear.

Logicube Talon® Software Update

Note: Make sure the update is running on the PC and the Logicube Talon® is connected to the host PC via the supplied parallel cable.

1. Press and hold the **START**/**STOP** button on the Logicube Talon® while inserting the power cord into the Logicube Talon® to bring up the Setup menu.
2. Scroll to the “Load SW from P. Port” option in the menu.
3. Press **SELECT** to UPDATE software and then follow the LCD on-screen prompts. The update will run for one to three minutes after which the Logicube Talon® will restart.
4. Press the **ABOUT** button to verify that the expected software version has been loaded.

12. Reference

Further Notes on Modes Available for the Forensic Talon®

Capture – Native or DD image

This process captures all data from the source drive to the destination drive. See the "**Anatomy of a Drive Capture**" section below for more information.

Drive Defect Scan

The Drive Defect Scan operation performs a surface scan of the drive media using the drive controller to verify the media. This is done without transferring any data from the drive and results in extremely fast operation at the maximum media speed of the drive. This is typically faster than the maximum sustained transfer speed of the drive. The media is scanned in blocks of 256 sectors. If a block fails to verify, it is retried once at the block level. If it fails again, each of the 256 sectors is scanned individually. Each sector is scanned up to ten times. If a sector fails immediately, it is classified as bad. If the sector fails to verify after a good read any time up to the tenth read it is classified as weak. If the sector is verified good for ten reads it is classified as good. If, after the individual sectors are all scanned and there are no bad sectors found, the block is classified as a weak Spot.

Options

Drive – Choices are Destination or Source

Speed – The choices are, Fast or Thorough

Printer – The print report option controls whether or not a hardcopy printout is automatically generated immediately following the operation.

The choices are YES, or NO.

Wipe Clean Destination

The Wipe Clean <WIPCLEAN DEST> function is the process that erases or wipes all existing information from the surface of destination disk drive.

Options

These are the user configurable options for the Forensic Talon® erase process.

Speed - The speed setting provides the option to set the speed at which an operation will be performed.

The choices are UDMA-5 to UDMA-0, PIO-AUTO, PIO-MED and PIO-SLOW.

Signature - A unique digital signature is written to the destination drive on the first sector of each logical cylinder boundary across the entire drive.

Choices are Yes or No

Printer - The print report option controls whether or not a hardcopy printout is automatically generated immediately following the operation.

The choices are Yes, or No.

Erase process with a source drive present.

The software first scans the source drive for a chunk of zero-filled sectors to use as a data source for erasing sectors on the destination drive.

If a chunk larger than 16 sectors is found, then the software will continue to erase the destination drive by streaming the zero filled chunk of sectors from the source drive to the entire destination drive.

If the software fails to find an acceptable chunk of zero-filled sectors on the source drive, then the software will inform the user and ask to continue the erase process without a source drive as described elsewhere. If the user declines then the erase process will abort.

Procedure

The Power-up and Initialization procedure for the erase process is identical to that previously described for the Capture process, except if the source drive is not detected, the erase process will continue instead of aborting.

Additional Commands

Verify

The Verify option adds an increased level of confidence in the capture process. The choices are: SHA-256, SHA-256 + V, MD5, MD5 + V and None.

SHA-256

This is the default setting for verification and uses special hardware to compute SHA-256 Hash values at an extremely fast and accurate rate.

NOTE: If the Destination drive has bad or weak sectors, this mode may not guarantee the accuracy of the SHA-256 Hash. If the destination drive's health is unknown, use the "+V" setting.

SHA-256 + V

This mode uses special hardware to compute SHA-256 Hash values at an extremely fast and accurate rate. It also performs a read-back and comparison of each block of data as it is captured. It is highly recommended that this mode be selected to ensure the accuracy of the SHA-256 Hash.

MD5

This setting uses special hardware to compute 128-bit MD5 Hash values at an extremely fast and accurate rate.

NOTE: If the Destination drive has bad or weak sectors, this mode may not guarantee the accuracy of the MD5 Hash. If the destination drive's health is unknown, use the "+V" setting.

MD5 + V

This mode uses special hardware to compute MD5 Hash values at an extremely fast and accurate rate. It also performs a read-back and comparison of each block of data as it is captured. It is highly recommended that this mode be selected to ensure the accuracy of the MD5 Hash.

None

This method performs no special verification and is used only for non-forensic cloning purposes.

On Error

The On Error option controls what actions are taken when the software runs into problem areas on the source drive. The choices are:

ABORT - The Abort option causes the software to stop the copying process and display an error message when an unreadable area is encountered on the source drive.

SKIP - The Skip option causes the software to ignore a bad sector and not copy it to the destination drive. All prior and subsequent sectors are copied while only the unreadable sector is skipped.

RETRY - The Retry option makes up to 50 attempts to reread an offending sector using the following sequence:

1. Reinitialize the source drive.
2. Dump the drive's cache buffer.
3. Reread the offending sector. If a good read occurs then the retry loop is aborted immediately and copying continues.

If the sector is still unreadable after the maximum number of retries, then it is skipped and the copying process continues with the following sectors.

RECOVER - At least one reinitialize and retry is performed for all choices before recovery is attempted. This prevents recoverable errors from halting the completion of the copying process. For all modes, except ABORT, the hardcopy printout will provide a list of sector numbers that failed.

The Recover option makes up to 50 attempts to reread an offending sector using the following sequence:

1. Reinitialize the source drive.
2. Dump the drive's cache buffer.
3. Reread the offending sector. If a good read occurs then the retry loop is aborted immediately and copying continues.
4. If the read failed, the low level code transfers the drive's buffer contents anyway. The buffer is examined and information is collected for a majority vote algorithm.

5. If the sector is still unreadable after the maximum number of retries, the software will then attempt to reconstruct the sector by applying a majority vote algorithm to the data collected while performing the retries. The sector is then written to the destination drive and the copying process continues with the following sectors.

Printer

The printer option contains a submenu with various functions controlling the generation of hardcopy printouts of Capture, DD Imaging, Scan or Wipe Sessions.

PRINT REPORT - The print report option controls whether or not a hardcopy printout is automatically generated immediately following a Capture, Scan, or Wipe session. The choices are YES, or NO.

PRINT LAST SESSION - The Print Last Session option enables the user to get a hardcopy printout of the previous Capture, Scan or Wipe session even if the Print Report option above was not enabled. As long as power remains applied to the unit, the previous session's results are available.

PRINT SEARCH DETAIL – Prints a detailed report of all words matched during the last session, and their absolute location

PRINT SEARCH TEXT – Prints a snippet of text before and after the matched word, for every word matched during the last session

EJECT PAGE - The Eject Page option is a utility function that will send a page eject or form feed command to the printer. This may be necessary when using certain kinds of laser printers.

Anatomy of a Drive Capture

The drive capture process implemented in the Forensic Talon® is a specific and detailed process designed to ensure maximum integrity and certifiable performance. It consists of a number of checks and procedures that are detailed in the following section.

Power-up and Initialization

Power and reset are applied to both source and destination drives, then the software waits for up to 30 seconds for the source drive to become ready.

When the source drive is ready, the software identifies the drive configuration and initializes drive parameters.

The software then checks the destination drive for ready status and waits, if necessary. When the destination drive becomes ready, the software identifies the drive configuration and initializes drive parameters.

If the initialization of either drive fails, the software aborts the process with an error message.

The software verifies that the destination drive capacity is equal to or greater than the source drive. If the destination capacity is insufficient, then the user is informed and the software will abort the capture process.

Log file name entry

The unit initializes the CF Drive, and then asks the user to enter a case name. This name must be 8 characters or less and use DOS naming conventions. The Log file name is used for the report that is created at the end of the capturing session and written to the CF Drive. The report can be opened and printed from any text editor in Windows (like Notepad).

Calibrate Transfer Speed

If the Speed option described previously is set to “UDMA-5”, then the calibration procedure is performed as follows:

1. The transfer speed is set to a conservative initial value.
2. A chunk of the source drive is copied to the destination drive.
3. If there are no errors, then the elapsed time is stored. If there is an error, then the software will set the transfer speed to a lower value and exit the routine.
4. The transfer speed is set to the next higher value and the process is repeated until the highest speed is reached that does not result in any errors.

Check Capture Integrity

This procedure tests the integrity of the data path including the following items.

- Drive interface
- Data cables
- Unit integrity
- Loose connectors.

The method used is as follows:

1. All bits of the data lines of the source drive are checked for toggling between one and zero while reading data from the drive. This is necessary because the data lines can be broken or unreliable and we can still communicate with and control the drive without transferring data.

   NOTE: For this test, the unit checks an 8 MB portion of the drive that starts 50MB from the start of the drive. If the drive is wiped, or there is no data in that area, then the unit will pause with an error: "**Source drive data lines can not be identified. Do you wish to continue?**" Choose <Yes> to continue with the Capture or choose <No> to abort. If the capture is continued, then the error message will not show up on the final capture report.

2. A chunk of the source drive is then copied to the destination drive at the speed previously set in the calibration procedure.
3. Every byte of every sector copied is then compared on the source and destination drives.
4. If the data on both drives match, then the software will exit the Integrity check and continue the capture process. If the data does not match, the transfer speed is lowered to the next available setting. The process is then repeated until the data is identical on each drive.

   NOTE: If a match does not occur, the unit will fail with an error.

Erase (WipeClean™)

This is used to erase all data on the target drives prior to a capture to remove any previously written data on those drives. It is highly recommended that the destination drive be erased in the lab before attempting a capture. From an evidential point of view, it removes doubt whether old data was leftover from a previous capture. Only the drive INSIDE the Forensic Talon® unit can be erased.

Erase Procedure

Power-up and Initialization

The Power-up and Initialization procedure for the erase process is identical to the Capture process, except if the source drive is not detected, the erase process will continue instead of aborting.

Erase process with a source drive present.

The software first scans the source drive for a chunk of zero-filled sectors to use as a data source for erasing sectors on the destination drive.

If a chunk larger than 16 sectors is found, then the software will continue to erase the destination drive by streaming the zero filled chunk of sectors from the source drive to the entire destination drive.

If the software fails to find an acceptable chunk of zero-filled sectors on the source drive, then the software will inform the user and ask to continue the erase process without a source drive. If the user declines then the erase process will abort.

Erase process without a source drive present.

The software will write zero-filled sectors directly to the entire destination drive using programmed I/O. This is the slowest and least desirable mode of operation.

Security Erase Process

The Talon accesses the Destination drive and determines whether or not it supports Security erase Mode. If supported, the Talon will send “Security AT” commands to the Destination drive instead of copying a pattern of zeroes. This procedure runs at cloning speed and supports writing the Signature. During a Security Erase, the progress bar will show time elapsed as well as time remaining.

NOTE: Security Erase mode can only be used in **WipeClean Dest.** Mode. It is not supported in Native Capture mode.

Write a unique signature to the destination drive.

By default, the software writes a unique digital signature to the destination drive on the first sector of each logical cylinder boundary across the entire drive. This enables the Capture process to quickly verify that the destination drive has been erased prior to the Capture process. The unique signature is written to the last 12 bytes of the sector. The data pattern is

0xAAAA, 0x5555, followed by the character string “Logicube”.

If needed, the user can disable the signature by selecting “NO” on the “Signature” menu located beneath the wipe mode.

Verify Erasure

The destination drive is checked to be sure it has been erased before copying the data from the source to the destination drive. Verifying the existence of a unique digital signature that is written to the drive during the Wipe-clean or erase function performs this check. The signature is written periodically across the entire drive when the Forensic Talon® erases it. If the drive is verified as erased, then the Capture process will proceed without any user intervention. If the erase is not verified, the user is asked if the drive should be erased now. If the user says yes, then the drive is erased and the Capture process will proceed. If the user declines, then this is noted and will show on the printed report. The Capture process will proceed.

Capture Source Drive Data To Destination Drive

All Data on the source drive is copied sector-by-sector to the destination drive.

Check for Erasure of Unused Portion of Destination Drive

If the destination drive has not been previously verified as erased and the source drive has less capacity than the destination drive, then the software will ask the user whether or not to erase the unused remaining portion of the destination drive. If the user accepts, then the remainder of the destination drive will be erased and the Capture process will continue. If the user declines, then this is noted and will show on the printed report. The Capture process will proceed. This is to ensure that there is no leftover data from any previous usage on the extra portion of the drive. Note: In the DD imaging modes, erasure of remainder of drive is not an option.

Print Final Capture Report

If the Printer setting was set to YES prior to Capture, then the unit will prompt the user with a message: “Make sure that the printer is connected, powered up and online. Press <OK> to print”. Press the Select button to initiate printing. A Final Capture Report will then be printed.

If this is the first time that the printer is used since the Talon® was powered up, a prompt will come up asking the user to choose “Pentax” or Standard”. Choose “Pentax” if the Pentax Pocketjet 200™ thermal printer is attached to the unit, otherwise select “Standard” for any other printer.

If the Printer setting was set to NO prior to capture, then a report can still be printed as long as the unit hasn’t been powered down, rebooted or used to clone more drives. Just press the Set Button, Scroll down to Printer, press the Select button, scroll down to “Additional Reports”, press Select again, highlight “Print Last Session” and hit Select.

A copy of the report is also written to the CF drive. It is named <Log file name>.LOG.

Final Capture Report (Hardcopy Printout)

The hardcopy printout available on the Forensic Talon® was designed to provide sufficient information for use as an evidence identification tag. It contains information on the unit used to acquire the evidence, the personnel acquiring the evidence, and the important information for the actual Capture session.

Information Format

This section describes the information format that appears on the Forensic Talon® hardcopy printouts. For an example, see the included page at the end of this section.

Unit Information - The unit Information section identifies the model name of the acquiring unit, the unit serial number, and the software version installed.

Forensic Information - The Forensic Information section contains several lines for the user to enter the necessary information relevant to each investigation.

There are spaces for the following information:

- Evidence number and/or any alias identifier.
- The name of the person(s) acquiring the evidence.
- The date and time that the evidence was acquired.

- The location at the scene of the investigation where the evidence was acquired.
- A description of the acquired evidence.

Session Information - This section of the printout contains information specific to the actual Capture session.

Session Settings Information – This section contains information pertaining to the actual Session that is not specific to either drive. It contains the following:

- Operating Mode. This can be Capture, DD Capture, Scan or Wipe clean.
- Verify. This reflects the Verify option setting for each operating mode as explained in previous sections of this text.
- Speed. This reflects the Speed option setting for each operating mode as explained previously.
- Connection. This is the connection method for the operating mode. This is meant to indicate whether a direct IDE connection, USB, or Parallel Link was used for the operating mode.
- Results. This line appears on the hardcopy only if the operating mode was Capture. It will contain one of the following lines.
  - "A 100% MIRROR COPY OF THE DRIVE HAS BEEN SUCCESSFULLY EXECUTED!"
  - "SESSION RESULTS ARE INVALID BECAUSE THE OPERATION WAS ABORTED!"
  - "SESSION RESULTS ARE INVALID BECAUSE THE OPERATION WAS IN ERROR!"
- Extra information. This line appears on the hardcopy only if the operating mode was Capture. It will contain one of the following lines:.
  - The destination drive was verified as erased before Capture!
  - The destination drive was erased during the Capture!
  - Operator declined FULL destination drive erase and erased remainder.
  - Operator declined FULL and remainder destination drive erase.

Source drive Information - This section of the printout contains information specific to the source or Suspect drive. This will only appear if the operating mode was (Native) Capture or DD Image Capture with

Verify set to **256 or MD5 + Disk**. It contains the following:

- Drive Identification. These lines print the model and serial number as reported by the source drive.
- Physical Geometry. These lines indicate the number of cylinders, heads and sectors, the total number of sectors, and the drive size.
- 256/MD5 Value. This line prints the computed SHA-256 or MD5 value for the source drive.
- Error recovery information. These lines will only appear if the On Error setting for the Capture operation was set to something other than abort. If the setting was set to “skip”, then a single line containing the total number of skipped sectors will be printed.
  If the setting was “retry” or “recover”, two lines will be printed: One containing the total number of recovered sectors; one containing the total number of non-recovered or skipped sectors.

Destination drive Information - This section of the printout contains information specific to the destination drive. It contains the following.

- Drive Identification. These lines print the model and serial number as reported by the destination drive.
- Physical Geometry. These lines indicate the number of cylinders, heads and sectors, the total number of sectors, and the drive size.
- 256/MD5 Value. This line prints the computed SHA-256 or MD5 value for the destination drive. This will only appear if the operating mode was (Native) Capture with Verify set to **256 or MD5 + Disk**.
- Media Verify information. These lines will only appear if the operating mode was set to Scan. If after a Scan operation, any bad sectors, weak sectors, or weak spots are detected, then the addresses of those sectors are printed followed by the grand totals for each type.
- If one of the DD imaging modes was used with verify set to **256 or MD5 + File**, a list of file names with their respective SHA-256 or MD5 values will be printed at the bottom of the page.

Audit Trail Authentication Checksum – This number is used to verify that the report residing on the CF Drive has not been altered in any way. The Checksum is a proprietary Hash value.

Note: The Audit Trail Authentication Checksum value is not a standard MD5 Hash value and it will not match the value calculated by third-party software or other means.

Keyword List – If a keyword search was performed during the capture, a list of the found keywords will appear at the very end of the Final Capture report.

Example of Hardcopy Printout

```
*****     LOGICUBE TALON     Serial No.: 65535  Software: V2.12RC  *****

Evidence Number_____________________ Alias_____________________

Evidence Acquired by_____________________________________________

Evidence Acquired on_____________________ AT_____________________

Location at scene________________________________________________

Description______________________________________________________

                          SESSION SETTINGS

  Operating Mode: Capture           Address Mode: LBA
  Verify        : SHA-256+V             Speed    : UDMA-0
  Connection    : Direct

    100% MIRROR COPY OF THE DRIVE HAS BEEN SUCCESSFULLY EXECUTED!

    Operator declined FULL and remainder Destination Drive erase!

****************************   SOURCE DRIVE   ****************************

                      Physical Characteristics

  Drive Model: QUANTUM FIREBALL EX6.4A
      Serial: 276832824724

    Cylinders     Heads     Sectors     Total Sectors     Drive Size
       13328         15          63          12594960          6.0 GB

       Computed SHA-256 Value:
   CCDB70D9D29D0B0E94EEF14729D7EF45C54095BFC42EAEE01DE868FFCFDDC931
                        Skipped Sectors: 78

*************************   DESTINATION DRIVE   *************************

                      Physical Characteristics

  Drive Model: WDC WD400BB-23FJA0
      Serial: WD-WCAJC1500253

    Cylinders     Heads     Sectors     Total Sectors     Drive Size
       77536         16          63          78156288         37.3 GB

       Computed SHA-256 Value:
   CCDB70D9D29D0B0E94EEF14729D7EF45C54095BFC42EAEE01DE868FFCFDDC931
```

13. Frequently Asked Questions and Answers

Q. By comparison my Forensic Talon® appears to be operating slower than other units.

A. Make sure that your unit is using the latest software. Visit **http://www.logicube.com** and go to the support page to view the latest software level and if necessary download the software for your system.

Q. My Forensic Talon® continues to ask if I want to wipe a brand new capture HDD.

A. This is a normal question that will be asked unless the new HDD is wiped by the Forensic Talon™. Using the Forensic Talon® to prepare (pre-wipe) a new Destination HDD will eliminate this screen from displaying while on site thus speeding up the capture process.

Q. After installing a brand new destination drive in my Forensic Talon® and starting a capture, I received a message that the drive was not erased, is this normal?

A. Even though new drives are usually blank, they still need to be wiped to guarantee that they do not contain any data.

The Forensic Talon® writes a signature to the destination drive during the wipe session. It is this signature that tells the Forensic Talon® that the destination or capture drive was previously wiped.
Destination drives can be prepared ahead of time by wiping them with signature set to "YES".

Q. Can I make bootable "Clone" with the Forensic Talon®?

A. While the Forensic Talon® was not designed to produce bootable “clone”, it will create a copy of the source drive with bit-for-bit accuracy. Whether or not the destination drive will boot depends upon many factors that include drive geometry, operating systems, and PC BIOS issues.

Q. Capturing data from a Western Digital HDD is not working.

A. Most Western Digital drives require that the jumpers be removed for a capture to work. The exception to this statement is for the Western Digital "Xpert" series Hard Drives (an older manufactured version), where the jumper is set to the master position.

Q. I'm trying to update my Forensic Talon® with the latest software but I cannot get my PC to communicate with the unit.

A. The PC must be set up to communicate in the Bi-directional mode through the BIOS setup. Refer to your PC user manual. Also, you could try to update the unit using the Compact Flash card. Instructions on how to do that are available elsewhere in this manual.

Q. Will DD Image capture files have the same "odd sector" problem of the Linux operating system?

A. Although DD Image capture files are formatted as "DD Linux" files, they do not utilize the Linux kernel. The Linux OS is unable to see the last sector of a drive that has an odd number of sectors. Some users have asked if this problem will prevent the last sector of an odd sector drive from being captured. The answer is no.

14. Index

Technical Support Information

For further assistance please contact
Logicube Technical Support at: (**001) 818 700 8488 7am-5pm PST, M-F (excluding US legal holidays)**
or by email to **techsupport@logicube.com**